PROYECTO DE TRABAJO DE GRADO

RECOMENDACIONES DE SEGURIDAD PARA LOS SERVICIOS DE COMPUTACIÓN EN LA NUBE, A PARTIR DE LOS ESTÁNDARES Y MODELOS DE SEGURIDAD DE LA INFORMACIÓN

LUIS EDUARDO ARCILA BONFANTE

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C. MAYO DE 2019

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

1 INTRODUCCIÓN

Las grandes empresas cuentan con centros de datos y personal especializado que les permite afrontar los aspectos de seguridad, sin embargo, las PYME (Pequeñas y medianas empresas) pueden afrontar un reto mucho mayor al momento de decidir mantener en la infraestructura propia, sus servicios debido a los altos costos que esto puede demandar.

Con el fin de mejorar la gestión de los servicios, las empresas han requerido con mayor demanda la migración de la información, aplicaciones, plataformas, entre otros, a la computación en la nube, tanto así que Gartner pronostica un crecimiento en el mercado del 81% entre el 2018 y el 2022, cifra que representa 148.8 billones de dólares de ingreso en los servicios de computación en la nube (Gartner Inc., 2019). Lo anterior, es debido que este tipo de servicios ha brindado ventajas competitivas al mejorar la disponibilidad de los mismos en las organizaciones, así como, la reducción de los costos en su implementación, al no ser necesario la compra de infraestructura tecnológica, sistemas operativos, energía y canales de comunicación para la transmisión de datos.

Hecho que ha promovido la necesidad de creación de organizaciones con el fin de generar buenas prácticas para el aseguramiento de este tipo de servicios, como es el caso de Cloud Security Alliance (CSA), quienes evalúan aspectos y proponen recomendaciones respecto a la seguridad en la nube.

Es por este motivo, que se ha visto la necesidad de realizar un análisis de los criterios de seguridad recomendados a tener en cuenta al momento de contratar servicios de computación en la nube, una vez determinados dichos criterios se realizó una correlación con los estándares de seguridad con el fin de identificar el nivel de cumplimiento y así lograr generar recomendaciones a tener en cuenta al momento de implementar un servicio de computación en la nube. En este sentido, este documento a través de la revisión de los estándares, busca recopilar los aspectos más importantes a tener en cuenta con respecto a la seguridad en computación en la nube.

2 GENERALIDADES

2.1 LÍNEA DE INVESTIGACIÓN

El presente trabajo surge como un apoyo del proyecto de investigación denominado "Diseño de una arquitectura de seguridad de TI para cloud computing" que se encuentra inscrito a la línea de investigación "Software inteligente y convergencia tecnológica" y pertenece al programa de "Especialización de seguridad de la información" de la Universidad Católica de Colombia. En este sentido los objetivos propuestos en el presente trabajo se encuentran alineados con los insumos requeridos para el proyecto de investigación.

2.2 PLANTEAMIENTO DEL PROBLEMA

La computación en la nube, se entiende como los datos que están en el ciberespacio y que por su naturaleza son accedidos a través de Internet. Por este motivo, uno de los aspectos que causan mayor incertidumbre cuando se habla de computación en la nube es la seguridad, debido a la facilidad de su acceso haciendo uso de Internet.

En la actualidad, las empresas han incrementado el uso de los servicios de computación en la nube, debido a la oportunidad de disminuir los costos de mantenimiento de infraestructura propia. Dicho crecimiento ha generado una aumento de ataques a los servicios en la nube, como se evidencia en el reporte de (Alert Logic, 2017) y (PaymentsCM LLP, 2015), en la actualidad se ha visto un incremento significativo en la cantidad de ataques que se realizan a este tipo de servicios, tanto así que de septiembre 2018 a febrero de 2019 los ataques aumentaron un 65% según el estudio "Cloud Application Attack Snapshot: Q1 2019" (Rogers, 2019), a las infraestructuras que prestan este tipo de servicios, y es por esto que se evidencia la necesidad de identificar los aspectos a tener en cuenta en las empresas para los servicios de computación en la nube.

En este sentido, el análisis en este trabajo busca identificar a través de la revisión de los estándares y modelos internacionales relacionados con la seguridad en la computación en la nube,

los aspectos necesarios para salvaguardar los niveles de seguridad de la información de los datos tratados en la nube, con el fin de lograr determinar los controles mínimos a tener en cuenta al momento de la adquisición de este tipo de servicios.

2.2.1 Pregunta de investigación

¿Qué recomendaciones de seguridad se deben tener en cuenta en los servicios de computación en la nube, al analizar lo establecido en los estándares y modelos internacionales de seguridad?

2.3 JUSTIFICACIÓN

En las últimas décadas se ha observado una tendencia mundial hacia la computación en la nube, Gartner estima un crecimiento del mercado de la computación en la nube en 81% entre 2018 y 2022. Así mismo, Gartner indica conforme a los resultados obtenidos de las encuestas desarrolladas al sector, un tercio de las organizaciones mundiales tienen como una de las principales prioridades de inversiones la computación en la nube. Hechos que permiten determinar el gran crecimiento que se está observando de la adquisición de este tipo de servicios a nivel mundial. “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019”.

Al mismo tiempo que el mercado de la computación en la nube crece, la información expuesta por las organizaciones también aumenta, y así mismo, el interés de agentes externos por esa información. Por este motivo, surge la necesidad de buscar medidas para mitigar los riesgos asociados a la seguridad de la información en la computación en la nube, es por esto, que gobiernos y fundaciones a nivel mundial han enfocado sus esfuerzos en temas relacionados con la seguridad en la nube. Este es el caso de la organización “Cloud Security Alliance”, creada en 2008 luego del llamado de Jim Reavis para asegurar la nube durante el foro ISSA CISO en Las Vegas del mismo año.

Los estándares y modelos relacionados con el aseguramiento de la información en la computación en la nube afrontan aspectos de seguridad, tales como: gobierno de los datos, controles técnicos y responsabilidades contractuales. Sin embargo, muchos de estos estándares y modelos no son analizados desde una perspectiva diferente, que permita comparar los estándares

y modelos de seguridad contra los criterios de seguridad definidos en este trabajo.

Este trabajo pretende analizar e identificar los criterios de seguridad en la computación en la nube, teniendo como base, las buenas prácticas y modelos más utilizados en la actualidad, con el fin de abarcar desde otra perspectiva los distintos aspectos de seguridad de la información en la nube.

Los beneficios que se pueden llegar a obtener de este trabajo son identificar criterios y recomendaciones de seguridad que ayuden a las organizaciones a implementar la seguridad en la computación en la nube. Teniendo en cuenta lo anterior, este trabajo es una guía para las organizaciones que quieren adquirir servicios en la nube, planteando recomendaciones construidas a partir del análisis de las buenas prácticas, modelos y estándares de seguridad, con el fin de que puedan implementar esos servicios de manera segura.

2.4 OBJETIVOS

2.4.1 Objetivo general

- Plantear recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información.

2.4.2 Objetivos Específicos

- Definir los criterios de seguridad en la computación en la nube.
- Correlacionar los criterios de seguridad en la computación en la nube, con los lineamientos definidos en los estándares y modelos de seguridad de la información.
- Generar recomendaciones de seguridad en computación en la nube a partir de la correlación elaborada.

3 MARCOS DE REFERENCIA

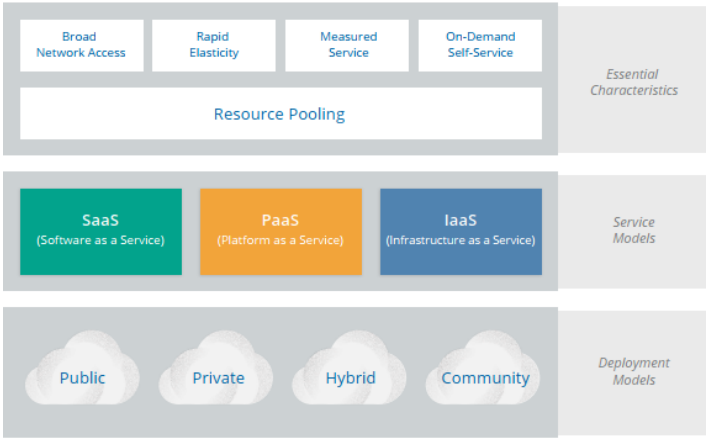
3.1 MODELO DE COMPUTACIÓN EN LA NUBE

A continuación, se describen los aspectos claves que se deben tener en cuenta para entender los servicios de computación en la nube y los tipos de nube, como se administran los servicios en la nube y como se pueden contratar estos servicios.

NIST es una organización del gobierno de Estados Unidos con amplia aceptación a nivel mundial; con el fin de hablar un lenguaje común con definiciones ampliamente utilizadas para computación en la nube, este trabajo se basa en las definiciones de su publicación "The NIST Definition of Cloud Computing" (NIST 800-145).

NIST 800-145 define la computación en la nube como un modelo para permitir el acceso a un conjunto compartido de recursos informáticos como redes, servidores, almacenamiento, aplicaciones y servicios, los cuales son configurables y asequibles de manera conveniente, bajo demanda y desde cualquier lugar de la red. Este modelo está conformado por cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue los cuales se explican a continuación.

Ilustración 1 Modelo de computación en la nube.



Fuente: (Cloud Security Alliance, 2017)

El modelo de computación en la nube propuesto por NIST explica las siguientes características esenciales:

Autoservicio bajo demanda: “On-demand self-service” hace referencia a que las capacidades contratadas son administradas por el cliente sin que se requiera de intervención humana con el proveedor.

Amplio acceso a la red: Todos los recursos están disponibles a través de una red, sin necesidad de acceso físico directo; La red no es necesariamente parte del servicio.

La agrupación de recursos: El proveedor de servicios en la nube abstrae los recursos físicos y los recopila en grupos virtuales, que pueden asignarse a diferentes clientes según lo requieran. Los clientes no tienen control sobre la ubicación exacta de los recursos proporcionados, pero pueden solicitar que sean ubicados en un centro de datos o país de su elección.

Rápida Adaptación: Permite a los clientes escalar rápidamente los recursos que requieren, lo cual puede realizarse de forma automatizada bajo algunas limitaciones preestablecidas entre las partes. Esto permite al proveedor ofrecer recursos como procesamiento, memoria, espacio en discos entre otros que se ajusten rápidamente a los requerimientos del cliente.

Medición de Servicios: La utilización de recursos en la nube es medida, controlada permitiendo que los sistemas optimicen los recursos, cuando esta información es informada brinda transparencia para los clientes y el proveedor.

El modelo de servicios en la nube propuesto por NIST tiene tres tipos de servicios los cuales son Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS). Los cuales se explican a continuación.

Software como Servicio (SaaS): Consiste en una aplicación administrada por el proveedor

y alojada en la infraestructura de este a la cual los clientes acceden desde un navegador web o una aplicación de cliente liviana. El cliente puede administrar configuraciones limitadas de la aplicación, el resto de la administración es responsabilidad del proveedor.

Plataforma como Servicio (PaaS): En este tipo de servicios se ofrecen plataformas de aplicaciones, desarrollo, almacenamiento y procesamiento para que el cliente ejecute sus aplicaciones. La administración de los servidores, redes e infraestructura es responsabilidad del CSP, pero el cliente tiene control sobre las aplicaciones y algunas configuraciones para el hospedaje de las mismas.

Infraestructura como Servicio (IaaS): El proveedor ofrece recursos de infraestructura, computación, red o almacenamiento, los cuales son administrados por él y controlados parcialmente por el cliente. El cliente administra los sistemas operativos, software y aplicaciones que utilicen la infraestructura contratada.

Los modelos de despliegue ofrecidos por el proveedor de servicios son Nube Privada, Nube Publica, Nube Hibrida y Nube Colectiva. Estos modelos se explican a continuación.

- **Nube pública:** Propiedad de una organización que vende los servicios de la nube a otras organizaciones
- Nube privada: Es de uso exclusivo de una organización que puede ser administrada por la misma empresa o terceros
- **Nube hibrida:** combina nubes públicas y privadas, manteniendo sus identidades, pero vinculando estas nubes como una unidad.
- **Nube Colectiva:** La infraestructura en la nube es utilizada exclusivamente por un grupo de organizaciones, relacionadas entre ellas por su misión, requisitos de seguridad, políticas, etc.

ISO/IEC 17788:2014 además de los servicios definidos por NIST aborda otros desde un punto de vista más granular, ejemplo de ello son Computo como Servicio (CaaS) y

Almacenamiento de Datos como Servicios (DSaaS) que por sus características pueden enmarcarse dentro de los propuestos por NIST. A continuación, se presenta una tabla que correlaciona por sus características los servicios ISO/IEC y los de NIST.

Tabla 1Definicion del modelo de servicios ISO/IEC contra NIST

Definiciones ISO/IEC	**Definiciones NIST**		
Servicios	**IaaS**	**PaaS**	**SaaS**
Infraestructura como Servicios	X	-	-
Plataforma como servicio	-	X	-
Software como Servicio	-	-	X
Computo como Servicio	X	-	-
Almacenamiento de datos como Servicio	X	X	X
Red como Servicio	X	X	X
Comunicaciones como Servicios	-	X	X

Fuente: (Propia)

Cloud Service Provider (CSP) y servicios en la nube.

Los proveedores de servicios en la nube (CSPs) son organizaciones que ponen a disposición de sus clientes parte de su infraestructura, canales de datos, personal, centros de cómputo y otros recursos necesarios para brindar a sus clientes servicios en la nube.

Application Program Interface (API)

La Interfaz de Programación de Aplicaciones (API) es un conjunto de funciones que permiten a los desarrolladores de aplicaciones interactuar entre varios aplicativos, sistemas operativos o productos informáticos; las APIs permiten acelerar el desarrollo ya que los desarrolladores no deben reescribir código para conectarse con otras aplicaciones.

En la nube se utilizan APIs para facilitar la comunicación entre aplicativos web y funcionalidades del software en la nube, sin embargo, pueden representar un riesgo de seguridad

si no han sido desarrolladas teniendo en cuenta estándares de seguridad y buenas prácticas.

3.2 BUENAS PRÁCTICAS Y MODELOS DE SEGURIDAD

3.2.1 BUENAS PRACTICAS

Las buenas prácticas para proteger el entorno de la información proveen a las organizaciones de herramientas para defender sus activos, en el entorno de la nube las organizaciones ven expuestos sus activos a nuevas amenazas las cuales deben ser abordadas desde un análisis de riesgos. Con el fin de asegurar la información en la nube, las organizaciones pueden utilizar como guía las buenas prácticas que se describen a continuación.

3.2.1.1 U.S. Department of Homeland Security – Cloud Security Guidance .gov Cloud Security Baseline 2018.

El Departamento de Seguridad Nacional de los Estados Unidos, mediante el documento "Cloud Security Guidance .gov Cloud Security Baseline" de 2018 brinda una línea base de seguridad en la nube con el fin de comprender y abordar los riesgos y desafíos asociados con la protección de datos y aplicaciones en la nube. Dicho documento logra identificar algunas consideraciones junto con el motivo por el cual cada una es importante para logara un aseguramiento de la información en la computación en la nube, al igual que las medidas que se deben implementar para mitigar los riesgos asociados. A Continuación, se realiza un resumen de los aspectos más importantes identificados en "Cloud Security Guidance .gov Cloud Security Baseline 2018".

Corte de servicio del proveedor de la nube. Los proveedores deben contar con un plan de contingencia que permita a las organizaciones seguir operando cuando una interrupción del servicio ocurra.

Modelo de negocio en la nube. Existen casos históricos en que un CSP, Proveedor de servicios en la nube, por sus siglas en inglés, ha cambiado su modelo de negocio o incluso ha salida

del negocio sin poca o ningún aviso previo, por lo tanto, se deben resguardar los datos en la nube y se deben establecer planes para la transferencia de los servicios en la nube de un proveedor a otro.

Bloqueo del proveedor en la nube. Este aspecto hace referencia a la dependencia que existe entre las organizaciones y el CSP, en casos en los que se requiere cambiar de proveedor de servicios en la nube los costos y herramientas requeridas para dicha migración pueden llegar a hacer inviable el cambio, por tal motivo se debe contar con una estrategia de migración que minimice los efectos negativos cuando se requiera un cambio de CSP.

Dependencias desconocidas del CSP. Los CSPs pueden contratar servicios con otros proveedores y no necesariamente informarlo a sus clientes, por lo tanto, es importante que las políticas de seguridad también sean cumplidas por terceros ya que estos pueden convertirse en un vector de ataque desconocido.

Falta de conocimiento y control sobre la cadena de suministro. Los CSP pueden contratar a terceros que requieran acceso privilegiado a componentes de los servicios que se contratan y estos pueden ser susceptibles a manipulación, malware, spyware, calidad, etc.

Complicaciones en la gestión de parches y versiones. Las actualizaciones y parches son esenciales para la estabilidad, seguridad y rendimiento de los sistemas por lo tanto es importante monitorear y supervisar la instalación de actualizaciones y parches que apliquen a los servicios contratados en la nube.

Pérdida de control sobre los datos. Los datos almacenados en la nube son susceptibles a perdida, ya sea intencional, accidental o por catástrofes naturales la protección de los datos no es solo responsabilidad del CSP, sin embargo, este último es el encargado de implementar las medidas de seguridad para proteger los datos y los métodos de recuperación.

Mayor potencial para la mala configuración de los servicios de seguridad. En la computación en la nube se requiere capacitación adicional, ya que no basta con implementar las

medidas de seguridad y configuraciones para proteger los sistemas, sino que también se deben comprender los controles de seguridad, interfaces, aplicaciones y vulnerabilidades en la nube.

Incapacidad para verificar la eliminación de datos. En la nube los clientes difícilmente tienen un alto nivel de trazabilidad desde que los datos son creados hasta que estos se eliminan, por lo tanto, se debe tener en cuenta las dificultades para la eliminación de datos en la memoria RAM, en discos donde se analizan y computan y copias de respaldo que se pudieron haber realizado de estos.

Falta de control sobre la gestión de la seguridad física. Los clientes tienen una limitada administración de los controles de seguridad física para proteger los sistemas, ya que a menudo el CSP es el responsable de esto, y no necesariamente cumple con las especificaciones requeridas o deseadas para prevenir el acceso físico no autorizado a la infraestructura.

Almacenamiento extranjero de datos. Los CSP pueden almacenar los datos de los clientes en diferentes países, y la jurisdicción de estos datos corresponde a la del país donde residen por lo tanto puede ser necesario solicitar que los datos se almacenen solo en determinados países con el fin de no incumplir con leyes de derechos de autor u otras normativas o por seguridad.

Coordinación con el CSP para el cumplimiento de las leyes y regulaciones. Los clientes deben cumplir con medidas de seguridad y otros controles, por lo tanto, se deben realizar reuniones con el CSP para validar que se cumplan las normativas y regulaciones que debe cumplir el cliente.

Adquisición extranjera de CSP. Un CSP puede ser comprado por persona, empresas o gobiernos con interés en los datos que se encuentran alojados en la nube, pudiendo obtener así acceso a ellos.

Mayor complejidad y carga en el personal de TI. El personal que migra los datos debe ser capacitado para garantizar que en la nube se mantenga la integridad, confidencialidad y disponibilidad de la información, de otra manera malas configuraciones en el nuevo entorno

podrían poner en riesgo los datos.

Mayor potencial para amenazas internas. Por su naturaleza, los servicios ofrecidos por el CSP requieren otorgar privilegios de acceso a sus empleados y terceros, por tal motivo se aumenta el riesgo de acceso, transferencia, modificación, eliminación de los datos no autorizado. Es por esto que el cliente y el CSP deben trabajar en equipo para detectar y mitigar estas amenazas.

Pérdida de Gobierno sobre los Activos. Cuando una organización coloca sus activos en la nube pierde gobierno sobre estos, por lo tanto, se debe establecer un modelo de responsabilidad compartida, con el fin de comprender los controles requeridos en el nuevo entorno y definir el cumplimiento de los mismos.

Administradores desconocidos. Los administradores de los servicios en la nube deben tener el perfil, la capacitación y la confiabilidad que garantice los estándares de seguridad requeridos por el cliente.

Mayor probabilidad de comprometer API. La interfaz de programación de Aplicaciones (API) son utilizadas para administrar e interactuar con los servicios en la nube, las APIs externas pueden tener vulnerabilidades por este motivo deben ser desarrolladas de manera segura, validadas, probadas y monitoreadas para garantizar que no sean vulnerables y utilizadas para afectar la seguridad de los datos y aplicaciones en la nube.

Reducción en la visibilidad y el control sobre activos y operaciones de seguridad. Las organizaciones propietarias de los datos pierden visibilidad y control sobre las capacidades y procesos de seguridad de los datos en la nube, ya que la infraestructura pertenece al CSP, puede no ser posible implementar mecanismos de monitoreo y control para prevenir la perdida de la integridad y confidencialidad de los datos.

Las organizaciones que contratan servicios en la nube deben tener presente el tipo de información que se almacena en ella con el fin de implementar los mecanismos de monitoreo y control de los activos que permitan salvaguardar la información.

Aprovisionamiento malicioso de recursos. Un atacante puede utilizar credenciales comprometidas o APIs vulnerables para acceder a recursos de infraestructura que le den mayor capacidad de computación para el ataque, pudiendo afectar la integridad, disponibilidad y continuidad del cliente u otras organizaciones.

Compromiso de Credenciales. El uso de credenciales comprometidas por un atacante es de mayor criticidad en la nube, ya que está expuesta a internet se deben tener en cuenta controles adicionales como doble factor de autenticación, reducir el número de credenciales con permisos elevados, funcionalidades para forzar el uso de contraseñas seguras, alertas y registros de eventos que permitan reforzar la seguridad de las credenciales.

Superficie de ataque aumentada debido a la tenencia múltiple. La tenencia múltiple hace referencia a que varios clientes del CSP pueden compartir recursos alojados en un mismo servidor físico. En caso de que un atacante logre comprometer una de las máquinas virtuales de un host físico, podría ganar acceso a este último comprometiendo a su vez todas las máquinas virtuales de ese servidor, indistintamente de la organización a la que pertenezcan.

Fuga de memoria en la infraestructura compartida. Este problema afecta la disponibilidad si la memoria no se libera adecuadamente por las aplicaciones, haciendo que los recursos de memoria no estén disponibles e incluso puede llegar a causar un bloqueo en el sistema informático. La confidencialidad puede afectarse si la memoria no es sanitizada correctamente antes de ser reasignada, permitiendo que se recuperen los datos escritos por el usuario anterior como credenciales de acceso.

Capacidad reducida para realizar pruebas forenses posteriores al evento. El análisis forense digital puede requerir acceso a infraestructura o hardware de la cual el cliente no es propietario, el CSP no permitirá realizar procedimientos forenses de hardware y software ya que podría afectar la seguridad y/o privacidad de otros clientes.

Pérdida de conciencia situacional por latencia inducida. Un cliente es consciente de una

situación tan rápido como pueda tener acceso a los registros de actividad y analizarlos, sin embargo, en la nube un CSP podría no disponer de esta información en tiempo real para sus clientes, por lo que el tiempo que transcurre desde que un evento es registrado y se toma conciencia de una situación es mayor en la nube.

Capacidad reducida para asegurar cargas de trabajo en la nube. Los servidores en la nube pueden ser utilizados para aprovisionar nuevos servicios sin que estos estén correctamente asegurados y monitoreados, en entornos como IaaS se pueden usar recursos de la nube que no están incluidos en el contrato causando efectos legales no deseados.

Ataques basados en la web. La nube es susceptible a ataques basados en aplicaciones web, APIs, cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, script injection, replay attacks, MIT, vulnerabilidades de los navegadores y vulnerabilidades no parchadas o no conocidas entre otros.

Amenaza Persistente Avanzada. Las APTs son difíciles de identificar ya que utilizan distintos vectores de ataque prolongados en el tiempo, analizan el tráfico para no levantar sospechas y pueden utilizar vulnerabilidades de día cero. Por lo tanto, las organizaciones deben asumir que serán atacadas y adoptar un enfoque de seguridad basado en defensa en profundidad (defense-in-depth). Las organizaciones y los CSP deben trabajar en conjunto para habilitar los Firewalls, la segmentación, el cifrado, el monitoreo y las capacidades de detección que permitan proteger mejor sus activos.

Denegación de servicio. Los ataques de DoS en la nube guardan relación con otros ambientes, sin embargo, por las características de la nube, un ataque a un SaaS podría afectar a varias organizaciones, aunque no sean el objetivo del ataque.

Información de ataque incompleta. Cuando se producen ataques en la nube el CSP será intermediario al entregar la información del ataque a las organizaciones afectadas, este role juega en contra para las organizaciones ya que les dificulta tener transparencia y veracidad sobre la completitud de la información suministrada por el CSP y por lo tanto comprender completamente

el ataque. Pueden existir escenarios en los que el CSP bloquee ataques y otros en los que se materialice, en ambos casos puede que no se informe a todos los clientes afectados, incluso aunque sean informados esta información puede estar incompleta, ser un informe de nivel gerencial o no tener incluidos todos los detalles.

3.2.1.2 Cloud Security Alliance – Security Guidance For Critical Areas of Focus in Cloud Computing v4.0

Cloud Security Alliance (CSA) ha enfocado sus esfuerzos en documentar temas relacionados con seguridad en la nube desde el 2008. CSA utiliza las definiciones de The "NIST Definition of Cloud Computing." (NIST800-145) y "Cloud computing - Overview and vocabulary" (ISO/IEC 17788:2014) con el fin de hablar un lenguaje común.

CSA establece trece (13) dominios que dan una guía a los usuarios para afrontar los problemas de seguridad en la nube, estos dominios están divididos en dos temáticas "Gobierno en la nube" y "Operación en la nube"; el primero hace referencia a orquestar los servicios en la nube para que brinden beneficios tangibles al negocio, mientras el segundo hace regencia a los aspectos necesarios para mantener operativos los servicios en la nube.

Gobierno en la nube

Gobernanza y gestión de riesgos empresariales. Es la capacidad de una organización para gobernar y medir el riesgo empresarial introducido por la computación en la nube. Se debe tener en cuenta las consecuencias legales por incumplimiento de acuerdos y responsabilidades de las partes, la capacidad de las organizaciones para evaluar adecuadamente el riesgo de un proveedor en la nube, las responsabilidades de cliente y proveedor para proteger datos confidenciales y cómo las fronteras internacionales pueden afectar estos aspectos.

Asuntos legales, contratos y documentos electrónicos. Existen posibles problemas legales al usar la computación en la nube, como son los requisitos de protección para la

información y los sistemas informáticos, las leyes de divulgación de violaciones de seguridad, los requisitos reglamentarios, los requisitos de privacidad, las leyes internacionales, etc. los cuales deben ser tenidos en cuenta cuando se contratan servicios en la nube.

Gestión del cumplimiento y auditoria. El cumplimiento de políticas, normativas y la legislación se debe mantener y evaluar cuando se utiliza la computación en la nube. Cuando las organizaciones migran sus datos a la nube se pueden presentar problemas para evaluar el impacto ya que es un nuevo ambiente en el que podría requerirse un tratamiento especial para algunos tipos de dato con el fin de garantizar el cumplimiento de las políticas de seguridad internas y los diversos requisitos de cumplimiento normativos y legislativos.

Gobernanza de la información. Son las estructuras y controles organizacionales que se utilizan para garantizar que la seguridad de los datos en la nube se encuentra alineada con los objetivos del negocio y requisitos de seguridad. Es importante establecer responsabilidades y empoderar a quién es responsable de la confidencialidad, integridad y disponibilidad de los datos para garantizar la gobernanza de la información.

CSA recomienda tener en cuenta los siguientes puntos para la gobernanza de la información en la nube:

- Revisar las políticas y estándares corporativos, teniendo en cuenta requisitos legales y reglamentarios y obligaciones contractuales, con el fin de realizar los ajustes necesarios para que los datos sean manejados por un tercero.
- Utilizar los controles de seguridad y contractuales para asegurar que las políticas y el gobierno corporativo cobijan los datos en la nube.
- De ser necesario modelar el manejo y controles de los datos, esto permite tener una visión clara del ciclo de vida de los datos y su comportamiento en la nube.
- La migración en la nube usualmente requiere algunos cambios en canales de datos, equipos, servidores, etc., de ser posible aprovechar estos cambios para repensar y reestructurar la infraestructura existente teniendo presentes buenas prácticas.

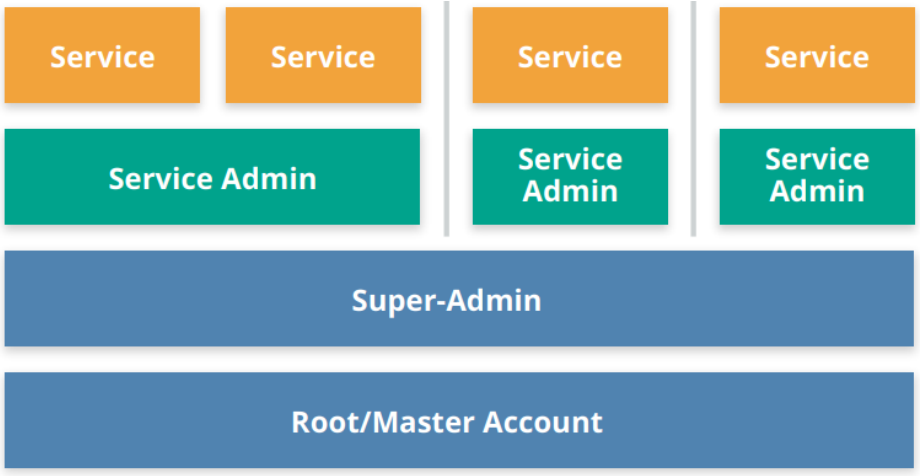
Operación en la nube

Plano de gestión y continuidad de negocios. Al utilizar servicios en la nube se abstrae y centraliza la gestión administrativa de recursos, los recursos de la nube se administran a través de APIs y consolas web accesibles a través con un conjunto de credenciales, por lo tanto, deben existir controles de seguridad adecuados para limita el acceso y lo que se puede realizar con este.

El plano de gestión de la nube se encarga de administrar los activos en la nube, mientras que los usuarios determinan cómo se configuran esos activos. El CSP es responsable de brindar mecanismos de accesibilidad y un ambiente de administración seguro, con funciones de seguridad que permitan configurar de manera específica lo que puede realizar cada usuario. Los usuarios son responsables de asegurar y administrar las credenciales de acceso y configurar correctamente los derechos de acceso.

Las cuentas de administración con mayores privilegios deben contar con múltiple factor de autenticación (MFA) y de ser posible también deben contar con esta característica las credenciales de usuarios menos privilegiadas con acceso al plano de gestión.

Ilustración 2. Plano de gestión: Cuentas de usuarios y servicios.



Fuente: (Cloud Security Alliance, 2017)

La continuidad del negocio y la recuperación de desastres tiene tres aspectos a considerar en la nube, estos son:

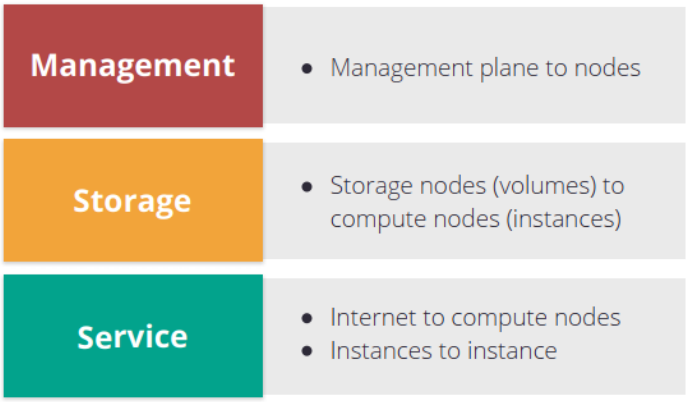
- Asegurar la continuidad y recuperación de los servicios del proveedor en la nube.
- Preparación y gestión de intermitencias de los servicios del proveedor en la nube, incluyendo el escenario en que los planes de recuperación de desastres del proveedor puedan fallar.
- Evaluar opciones para la migración de los datos en la nube a otros proveedores o plataformas.

Seguridad en infraestructura. La seguridad de la infraestructura es el principal requisito para operar de manera segura en la nube, incluye las consideraciones seguridad informática y de redes, seguridad de la carga de trabajo de la infraestructura y nube híbrida.

En la nube siempre utiliza algún tipo de virtualización que permite tomar los recursos físicos y agruparlos en recursos virtuales. Por lo tanto, la infraestructura en la nube abarca dos aspectos: los recursos fundamentales (hardware físico y su software) utilizados para crear los grupos de recursos de la nube y la infraestructura virtual que utiliza los grupos de recursos.

En la nube la red también es abstraída por seguridad y aislada mediante hardware dedicado, por este motivo se tienen los siguientes tipos de red: red de gestión para el tráfico del plano de administración, red de almacenamiento para conectar el almacenamiento virtual a las máquinas virtuales y la red de servicios para la interacción entre máquinas virtuales. A continuación, se ilustran los tipos de red en la nube.

Ilustración 3. Redes subyacentes en IaaS.



Fuente: (Cloud Security Alliance, 2017)

La infraestructura en la nube es susceptible a la sobrecarga de trabajo, este exceso de procesamiento puede ocasionar lentitud o bloqueos. El software y algunas herramientas de seguridad pueden no estar optimizados para trabajar en la nube lo que puede ocasionar mayor carga de trabajo en la nube. Los administradores deben ser conscientes de las limitaciones y capacidades para configurar las cargas de trabajo adecuadamente.

Cuando se realizan pruebas de vulnerabilidad y penetración en la nube se deben conocer y respetar las limitaciones de CSP, e informar de estas pruebas con anticipación ya que se pueden afectar servicios de otros clientes en la nube.

CSA recomienda conocer la seguridad de la infraestructura del proveedor, quien debe garantizar que las capas físicas, de abstracción y de orquestación de la nube sean seguras, revisar el cumplimiento de estándares y certificaciones y verificar de manera periódica que el CSP cumple con las buenas prácticas y regulaciones de infraestructura.

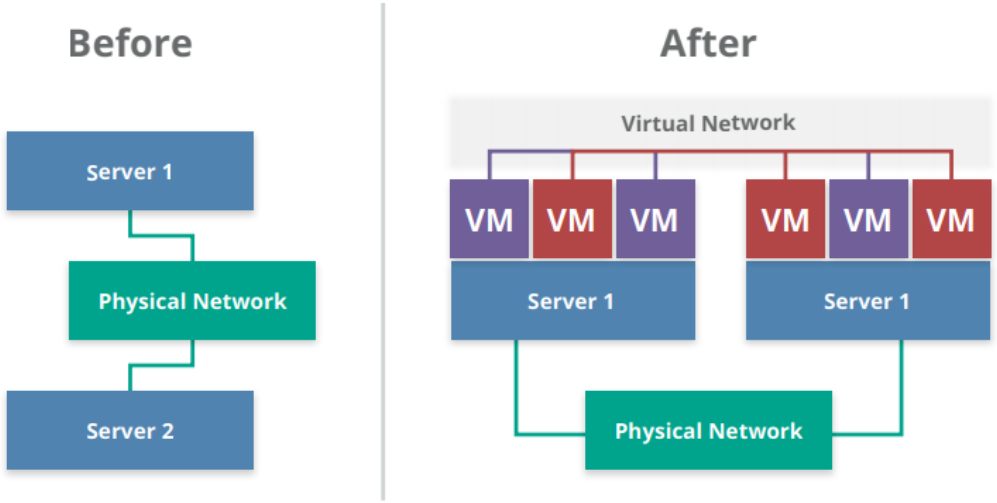
En cuanto a las redes, de preferencia se deben utilizar redes definidas por software (SDN), segmentar las redes virtuales para obtener un aislamiento, utilizar la regla de denegación por

defecto en los firewalls de la nube, utilizar los firewalls por carga de trabajo y no por tráfico de red, restringir el tráfico entre cargas de trabajo en la misma subred y evaluar uso de dispositivos virtuales que puedan causar cuellos de botella y disminuir el rendimiento de la red.

Virtualización y contenedores. La computación en la nube se basa en la agrupación de recursos físicos y la abstracción de estos (virtualización), este hecho agrega dos capas adicionales de seguridad para computación en la nube: la seguridad de la tecnología de virtualización (seguridad del hipervisor) y controles de seguridad para activos virtuales.

Cuando se utilizan tecnologías de virtualización se deben tener consideraciones adicionales en cuanto a monitoreo y filtrado de tráfico, en un ambiente virtual no necesariamente los datos salen del host físico y por lo tanto podrían no ser captados por las herramientas de monitoreo y filtrado. Esta situación se ilustra a continuación.

Ilustración 4. Flujo de datos en red física y en la nube



Fuente: (Cloud Security Alliance, 2017)

Los contenedores son una tecnología de virtualización que permite eliminar la necesidad de instalar un nuevo sistema operativo en el huésped, esto se debe a que los contenedores utilizan el núcleo del sistema operativo del anfitrión, obteniendo beneficios en almacenamiento,

procesamiento y carga del sistema. El aislamiento es gestionado por el software del contenedor permitiendo que el sistema operativo y recursos físicos del sistema sean compartidos mientras se aíslan las aplicaciones.

Las responsabilidades en el ámbito de la virtualización recaen en proveedor de servicios en la nube para asegurar la infraestructura física y la plataforma de virtualización, mientras que el cliente es responsable de implementar los controles de seguridad disponibles y comprender los riesgos asociados con el proveedor.

Respuesta a incidentes. Los procedimientos establecidos por las organizaciones para responder ante incidentes de seguridad deben adaptarse cuando los datos se encuentran en la nube. Es importante establecer las responsabilidades y alcance en las cuatro fases del ciclo de vida de un incidente:

- Preparación
- Detección y análisis
- Contención, erradicación y recuperación
- Post-Mortem

Se deben garantizar los elementos que permitan un manejo adecuado de incidentes y análisis forense durante las fases del ciclo de vida, de esta manera se podrá cumplir con el alcance acordado entre proveedor y cliente cuando un incidente ocurra.

Algunas de las recomendaciones en cuanto a la respuesta a incidentes son mantener un monitoreo continuo de los servicios en la nube, almacenar los datos que puedan servir como insumo para las fases del incidente en un lugar aislado al cual se tenga acceso durante el incidente y de ser posible que cumplan con los requisitos para realizar una cadena de custodia, aprovechar la orquestación para una rápida respuesta, contención y recuperación de las aplicaciones, el plan de respuesta a incidentes debe contener por cada proveedor de servicios en la nube como se detectara y manejara el incidente, y los SLA con cada proveedor deben garantizar que se pueda

llevar a cabo el plan de respuesta a incidentes.

Seguridad en aplicaciones. Se debe asegurar el software de aplicación que se ejecuta o está siendo desarrollando en la nube. Esto incluye elementos tales como si es apropiado migrar o diseñar una aplicación para ejecutarse en la nube y, de ser así, qué tipo de plataforma de nube es la más adecuada (SaaS, PaaS o IaaS).

En la nube las aplicaciones en la nube deben tener en cuenta tres aspectos de seguridad:

- Ciclo de vida de desarrollo de software seguro (SSDLC): se debe considerar como la computación en la nube afecta las aplicaciones durante su ciclo de vida.
- Diseño y arquitectura: Se deben tener en cuenta las últimas tendencias en el diseño de aplicaciones que puedan aportar mejorando la seguridad de estas.
- DevOpsel y CI/CD: tanto Integración Continua/Despliegue continuo (CI/CD) como DevOpsel son utilizadas para el desarrollo e implementación de aplicaciones y ofrecen oportunidades de mejora en la seguridad para las aplicaciones en la nube.

Seguridad de datos y cifrado. La seguridad de la nube debe estar basada en riesgos con el fin de garantizar que se asignen los recursos de manera adecuada. El cifrado del tráfico debe realizarse teniendo en cuenta la seguridad de los dispositivos.

Existen distintos mecanismos para almacenamiento de datos, en la nube es común utilizar la dispersión de datos “fragmentation of bit splitting” el cual toma los datos los fragmenta y ubica varias copias de ellos en distintas ubicaciones físicas. Este mecanismo provee a los datos de una alta disponibilidad y durabilidad, ya que los datos no se encuentran en un solo lugar.

Para asegurar los datos en la nube se deben tener conocer las capacidades que ofrece la plataforma en la nube que se está utilizando, se pueden crear matrices de perfiles y permisos de acceso para determinar los controles de acceso.

Con respecto al monitoreo de datos en SaaS, evalué el uso de un agente de acceso y seguridad en la nube (CASB), mientras que para servicios IaaS y PaaS puede ser más efectivo el uso de controles y políticas de seguridad en datos.

En cifrado y almacenamiento deben evaluarse las opciones ofrecidas por el proveedor, y utilizar claves gestionadas por el cliente de ser posible. Para lograr un adecuado uso de las técnicas de cifrado y gestión de clave se deben tener en cuenta las normas NIST SP-800-57, ANSI X9.69 y ANSI X9.73.

Verificar que las APIs y el monitoreo de datos ofrecidos por el proveedor cumplan con los requisitos de seguridad y con la política de ciclo de vida.

Gestión de identidad, permisos y acceso. En la nube la gestión de identidades, permisos y accesos (IAM) tiene consideraciones adicionales, el principal factor es que la gestión de la IAM debe ser compartida entre el proveedor y el cliente, por este motivo se requiere de un alto nivel de confianza y una clara asignación de responsabilidades.

Algunas recomendaciones a tener en cuenta son gestionar las identidades haciendo uso de los servicios de directorio para proporcionar control de acceso, se debe utilizar múltiple factor de autenticación (MFA), evaluar la preparación de una organización para llevar a cabo la gestión de identidades, permisos y gestión de acceso (IdEA) basada en la nube.

Seguridad como servicio. Un proveedor puede proporcionar garantías de seguridad que pueden incluir la gestión de incidentes, certificación de cumplimiento y supervisión de identidad y acceso.

Tecnologías relacionadas. Las tecnologías establecidas y emergentes con una relación cercana a la computación en la nube, incluyendo Big Data, Internet de las cosas y computación móvil adicionan nuevos factores que deben ser tenidos en cuenta para mantener la seguridad de la información.

3.2.1.3 Common Criteria (ISO/IEC 15408)

Common Criteria es una recopilación de tres normas internacionales Trusted Computer System Evaluation Criteria (TCSEC) de U.S. del año 1991, Information Tecnology Security Evaluation and Certification Scheme (ITSEC) de Europa del año 1985 y Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) de Canadá del año 1993, el resultado fue un estándar internacional de seguridad en equipos documentado bajo la norma ISO/IEC 15408 en el año 1998. A continuación, se mencionan los criterios de seguridad evaluados en ISO/IEC 15408 que son conocidos bajo la norma como "Clases" como se explica a continuación.

Requisitos funcionales de seguridad. Los requisitos funcionales se agrupan en clases, los miembros de una clase comparten una misma perspectiva o enfoque de seguridad, a continuación, se mencionan las 11 clases de Requisitos funcionales de seguridad.

- Auditoría
- Identificación y Autenticación
- Utilización de recursos
- Soporte criptográfico
- Gestión de seguridad
- Acceso al producto
- Comunicaciones
- Privacidad
- Ruta / Canales de confianza
- Protección de datos de usuario
- Protección de las funciones de seguridad del producto

Garantías de Seguridad. Al igual que los requisitos funcionales se agrupan en clases, cada una con un enfoque de seguridad, las ocho clases se mencionan a continuación.

- Administración de configuración

- Documentos de orientación y manuales
- Evaluación de vulnerabilidad
- Entrega y operación
- Soporte de ciclo de vida
- Mantenimiento de aseguramiento
- Desarrollo
- Prueba

3.2.2 MODELOS

Los modelos son la representación simbólica de la política, por este motivo son de gran importancia para el diseño y análisis de sistemas seguros; son representados en idea analíticas utilizando fórmulas matemáticas que son utilizadas por los programadores para implementarlas en el código de programación.

Las políticas de seguridad contienen un objetivo que se debe lograr, pero no especifican como, por su parte, el modelo brinda una solución el problema de seguridad planteado en la política. Un modelo toma una política abstracta que debe cumplirse, la analiza como un requisito y proporciona las fórmulas matemáticas, secuencia lógica e instrucciones de programación que deben llevarse a cabo para cumplir este objetivo.

A continuación, se explican los modelos de seguridad que se han desarrollado para implementar las políticas de seguridad:

3.2.2.1 Modelo de máquinas de estado

El estado de un sistema es una instantánea de un sistema en un determinado momento y contiene los permisos e instancias de los sujetos que acceden a objetos, este estado puede cambiar por distintas situaciones; el modelo de máquinas de estado consiste en tomar un sistema que inicia en un estado seguro, aplicar todas las posibles entradas o acciones para observar que transiciones

de estado son posibles y evaluar si el estado del sistema puede cambiar a un estado inseguro, si el estado permanece seguro después que ocurran todas las posibles acciones se dice que el sistema ejecuta un *modelo de máquinas de estado seguro*.

3.2.2.2 Modelo Bell-LaPadula

Los sistemas que utilizan este modelo se conocen como sistemas de seguridad multinivel, fue desarrollo para evitar el acceso no autorizado a información secreta para el gobierno de EEUU. Este modelo parte del hecho de que un sistema puede ser utilizado por diferentes usuarios cada uno con diferentes permisos, por lo que los datos se clasifican en diferentes niveles, de esta manera se puede controlar como deben interactúan los sujetos con cada objeto (lectura, escritura o lectura/escritura). En este modelo existen algunas reglas con el fin de mantener secretos como secretos, si usuario tiene un nivel superior no puede modificar objetos de nivel inferior, solo puede modificar los objetos de su nivel, pero si podrá leer todos los de niveles inferiores.

3.2.2.3 Modelo Biba

Este modelo busca proteger la integridad utilizando niveles, su funcionamiento se basa en que los datos con mayor nivel de integridad no se mezclen con los datos de menor nivel de integridad y para esto define tres reglas básicas para su funcionamiento: un sujeto no puede escribir datos en un objeto con un nivel de integridad más alto, un sujeto no puede leer datos de un nivel de integridad más bajo y un sujeto no puede solicitar un servicio de mayor integridad.

3.2.2.4 Modelo Clark-Wilson

El modelo de Clark-Wilson plantea tres objetivos para mantener la integridad: evitar que los usuarios no autorizados realicen modificaciones, evite que los usuarios autorizados realicen modificaciones incorrectas y mantener la coherencia de los datos internos y externos. Su funcionamiento consiste en que un usuario no es lo suficientemente confiable para que realice algunas aplicaciones es por esto que se necesitara un software que se encargue de autenticar el

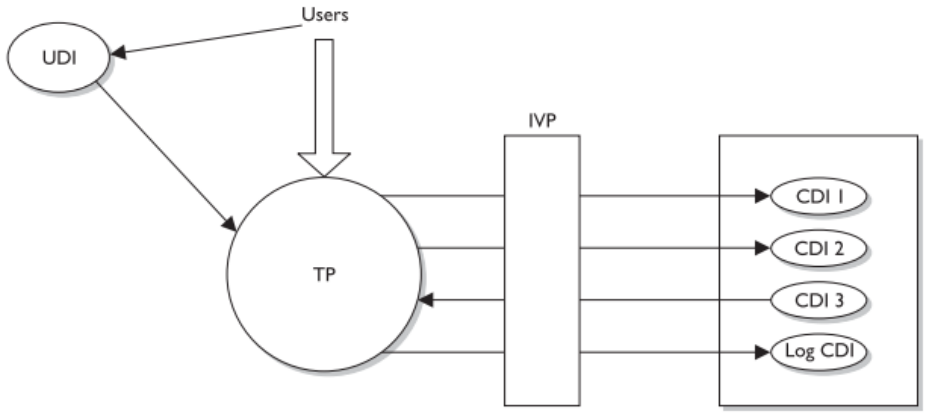
usuario y verificar que las acciones de este son válidas y permitidas; de igual manera debe existir un procedimiento de transformación para que realice los cambios por él y un procedimiento que garantice la consistencia de los datos para que correspondan a la realidad.

Con el fin de garantizar la integridad se definen cinco elementos los cuales se explican a continuación:

- Usuarios: Agentes que desea realizar una acción
- Procedimientos de transformación (TP): se encarga de realizar los cambios que solicita el usuario y consiste en operaciones abstractas programadas, como leer, escribir y modificar.
- Elementos de datos restringidos (CDI): elementos que solo pueden ser leídos o modificados por un TP.
- Elementos de datos sin restricciones (UDI): Elementos que pueden ser manipulados por los usuarios mediante operaciones de lectura y escritura
- Procedimientos de verificación de integridad (IVP): Son procedimientos que permiten verificar la consistencia de los CDI con el fin de mantener la integridad de los datos.

A continuación, se presenta un esquema de este modelo:

Ilustración 5. Interpretación grafica del Modelo de Clark Wilson



Fuente: (Harris)

3.2.2.5 Modelo de flujo de información

El modelo de flujo de información permite a los arquitectos y desarrolladores garantizar que el software no permita que la información fluya de una manera que pueda poner en peligro el sistema o los datos. Este modelo permite entender como los datos fluyen entre la memoria, cache, CPU, discos, unidades externas, impresoras, etc. de tal manera que se garantice que canales ocultos que pongan en riesgo la seguridad de los datos.

Un canal encubierto es canal que los diseñadores no pensaron para el flujo de información pero que puede ser utilizado con este fin y por lo tanto no está controlado por un mecanismo de seguridad. Estos canales existen por alguno de los siguientes motivos: Supervisión inadecuada en el desarrollo del producto, implementación incorrecta de los controles de acceso dentro del software, la existencia de un recurso compartido entre dos entidades que no se controlan adecuadamente. Existen dos tipos de canales ocultos: almacenamiento y temporización, el primero cuando se utiliza un software para transferir los archivos, por y el segundo consiste en procesos que se comunican con otros procesos utilizando los tiempos que asigna la CPU para cada proceso.

3.2.2.6 Modelo de no interferencia

El modelo de no interferencia aborda la problemática de canales encubiertos y ataques de inferencia, está basado en la seguridad multinivel y consiste en que nada de lo que se haga un usuario de un nivel alto debe afectar o ser conocido por un usuario de nivel bajo, ya que si un usuario de bajo nivel conoce lo que realizó un usuario de alto nivel esto afecta su entorno podría deducir alguna información, este hecho en sí mismo es un filtrado de información y se conoce como inferencia. Este modelo también analiza los recursos compartidos que los usuarios utilizan y como se puede transferir información entre los diferentes niveles de seguridad.

3.2.2.7 Modelo Enrejado

Este modelo se define como un conjunto parcialmente ordenado con limites superior e

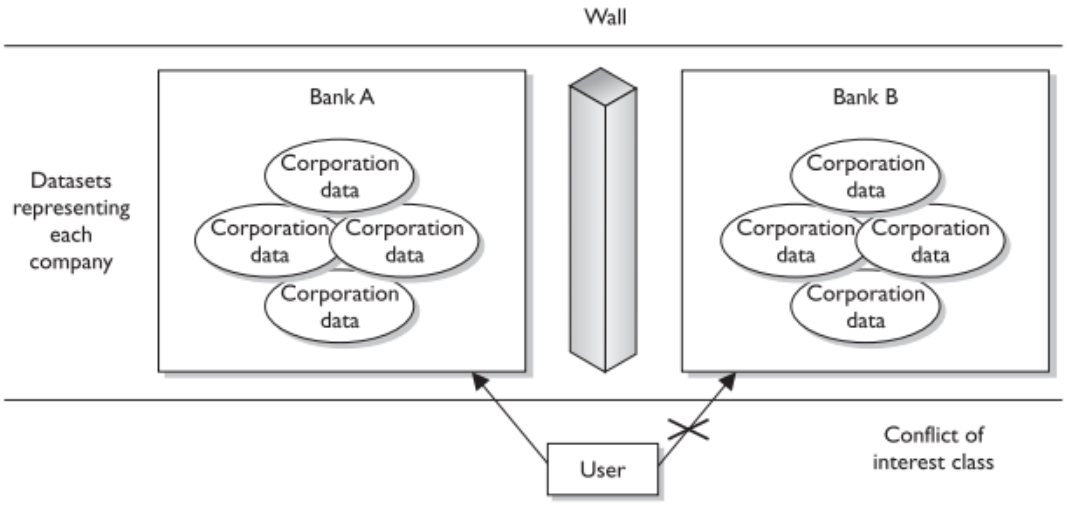
inferior, esta definición obedece a que se basa en etiquetas para los usuarios conocidos como conjunto y los objetos o archivos, “parcialmente ordenado” hace referencia a que el sistema debe interpretar las etiquetas del usuario y los objetos para determinar los permisos superiores e inferiores, estos límites son el permisos menos restrictivo como límite superior por ejemplo el usuario puede escribir y el límite inferior el más restrictivo por ejemplo el usuario puede escribir.

3.2.2.8 Modelo Brewer and Nash

Este modelo también es conocido como el modelo de “La Muralla China”, se basa en el modelo de flujo de información, pero adiciona el concepto de conflicto de intereses, permite implementar controles de acceso que cambian de manera dinámica según las acciones o permisos del usuario.

Este modelo aborda la problemática de conflicto de intereses cuando que la información de varios grupos, organizaciones, equipos, etc. se encuentra ubicada en un mismo repositorio, haciendo necesario un control que no permita que la información de un grupo sea accedida por miembros que no pertenezcan al mismo.

Ilustración 6. Interpretación grafica del Modelo Brewer and Nash



Fuente: (Harris)

Un CSP brinda una aplicación para acceder a reportes de ataques para sus clientes, un cliente solo debe tener acceso a sus reportes y por ningún motivo a reportes con información de otros clientes, ya que si son competidores en el mercado existiría un conflicto de intereses. A continuación, se presenta una explicación grafica de este modelo.

3.2.2.9 Modelo Graham-Denning

Este modelo complementa los modelos de Bell-LaPadula y Biba, ya que no abordan como se define y modifican los niveles de seguridad e integridad, para esto el modelo Graham-Denning define 8 principios:

- Cómo se crea de manera segura un objeto
- Cómo se crea de manera segura un usuario
- Como se elimina de manera segura un objeto
- Como se elimina de manera segura un usuario
- Como se otorgan de manera segura derechos de acceso de lectura
- Como se otorgan de manera segura derechos de acceso de eliminación
- Como se ceden de manera segura derechos de acceso
- Como se transfieren de manera segura derechos de acceso

3.2.2.10 Modelo Harrison-Ruzzo-Ullman (HRU)

Este modelo aborda los derechos de acceso de los usuarios y la integridad de estos, utilizando como base la simplificación de comandos que se requieren para realizar las operaciones de acceso a un objeto, en este mismo sentido se garantiza la integridad, porque si las operaciones se realizan con un solo comando y alguna de las sub-operaciones que se deben llevar a cabo falla, toda la operación es cancelada. De manera distinta sucedería si para implementar una operación deben realizarse las sub-operaciones A, B, C y D, si D falla A, B y C deberán volver a su estado inicial para mantener la integridad y por lo tanto esta no podría garantizarse.

3.2.3 ESTANDARES DE SEGURIDAD

Los estándares de seguridad permiten a las organizaciones entre otras cosas documentar, estructurar y organizar las actividades, controles y políticas, con el fin de que las organizaciones puedan implementar medidas para asegurar la información y mantener sus activos a salvo.

3.2.3.1 Common Criteria (ISO/IEC 15408)

Hoy en día "Common Criteria" es utilizado para la evaluación de características y propiedades de seguridad en sistemas y productos informáticos, en donde estos últimos reciben una calificación según los siete (7) niveles de cumplimiento conocidos como "Evaluation Assurance Levels" (EAL); los niveles con una numeración más alta dan mayor confianza en cuanto al cumplimiento de los requisitos de seguridad, a continuación, realiza una breve explicación de los niveles de evaluación.

EAL1: Hace referencia a que se ha "Probado funcionalmente" el producto. Se utiliza para identificar el correcto funcionamiento del producto, pero no considera otras amenazas de seguridad fuera de las funcionalidades del producto.

EAL2: Indica que se ha "Probado Estructuralmente" el producto. Se aplica cuando los desarrolladores o usuarios requieren evaluar la seguridad baja o moderada, en este nivel se requiere de la colaboración de desarrolladores, además de las pruebas realizadas en el nivel anterior se realizan pruebas de desarrollo, de vulnerabilidades u otras pruebas específicas más exhaustivas.

EAL3: Este nivel indica que el producto es "Metódicamente probado y comprobado". Se aplica cuando se requiere un nivel moderado de seguridad, en este nivel la colaboración de los desarrolladores es obligatoria, se realizan pruebas adicionales como el soporte del ciclo de vida, controles de entorno de desarrollo y la gestión de la configuración.

EAL4: El producto ha sido "Metódicamente diseñado, probado y revisado". En este nivel

la seguridad evaluada se considera entre moderada a alta, evalúa que al producto se le adicionado alguna ingeniería de seguridad en el desarrollo y es el nivel más alto para actualizaciones de productos. Los requisitos adicionales que son evaluados en este nivel son el diseño, implementación, análisis de vulnerabilidad, desarrollo y gestión de la configuración.

EAL5: El producto es "Semi-formalmente diseñado y probado". En este nivel la seguridad es alta y garantizada, requiere de un desarrollo planificado y con técnicas especializadas.

EAL6: El producto tiene un "Diseño verificado y probado Semi-formalmente". Se aplica cuando los activos son valiosos y en situaciones de alto riesgo, por lo que se requiere un entorno de desarrollo riguroso, en este nivel los riesgos de los activos justifican los costos adicionales de desarrollo. Se evalúan requisitos adicionales en el análisis, diseño, desarrollo, gestión de la configuración y análisis de vulnerabilidades de canal encubierto.

EAL7: El producto tiene un "Diseño Formalmente Verificado y Probado". Se aplica cuando los activos son valiosos y el riesgo es extremadamente alto, las garantías de seguridad se logran mediante la aplicación de métodos formales en pruebas y análisis.

Las características y propiedades de seguridad son evaluadas bajo dos atributos "Requisitos funcionales de seguridad" y "Requisitos de Garantía de seguridad", el primero hacen referencia a que un producto puede tener implementados mecanismos de seguridad como sería la autenticación, por lo tanto, el producto recibirá una calificación que es acorde al cumplimiento en seguridad de esta funcionalidad, sin embargo, si el desarrollo de esta funcionalidad no se realizó bajo parámetros exhaustivos, el cumplimiento de "Requisitos de Garantía de seguridad" recibirá una calificación más baja; de esta manera ambos atributos se complementan para brindar una calificación global que nos permite determinar el cumplimiento de la seguridad en productos y sistemas informáticos.

3.2.3.2 ISO 27001: Sistema de gestión de seguridad de la información.

El estándar ISO 27001 determina los requisitos, objetivos de control y controles requeridos para la implementación de un Sistema de Gestión de Seguridad de la Información, en donde, a

través de dichos parámetros, se busca lograr mitigar los riesgos de seguridad de la información a los cuales se encuentra expuesta una organización.

El estándar está compuesto por los requisitos mínimos que debería cumplir cualquier organización que quiera certificarse en la norma y busque mantener el mejoramiento continuo de su sistema de gestión de seguridad de la información, y de igual forma, propone en su Anexo A 114 controles para brindar las políticas, procedimientos y salvaguardas necesarias para proteger la información ante la materialización de riesgos de seguridad de la información.

3.2.3.3 ISO 27017: Código de práctica para los controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube

El estándar ISO 27017 internacional, proporciona directrices para la implementación de los controles de seguridad de la información en los servicios de la computación en la nube, planeando los escenarios de los clientes y proveedores de este tipo de servicio. Este estándar, se basa en las buenas prácticas de la seguridad de la información definidas en la ISO 27002, y complementa información con respecto a los controles propios de la computación en la nube.

La estructura del estándar, está presentado de manera muy similar a la ISO 27002, en donde se hace una revisión de cada uno de los objetivos de control y controles propuestos en este estándar. En los casos que se hace necesario ampliar la información con respecto a los clientes y/o proveedores, la misma es indicada en la descripción de cada control y se determina la especificidad del control respecto a la aplicación de la seguridad en la computación en la nube.

El estándar cuenta con dos anexos, en donde el primero presenta controles adicionales a tener en cuenta para los servicios de computación en la nube y el segundo, propone las principales amenazas tanto del cliente como del proveedor del servicio que pueda llegar a afectar la seguridad de la información.

Así mismo, el estándar se determina que, para la identificación adecuada de los controles,

se debe desarrollar con base en un análisis de riesgos, que me permita identificar los requisitos legales, contractuales y propios del servicio, con el fin de cumplir con los niveles de seguridad óptimos para la protección de la información a tratar.

4 METODOLOGÍA

4.1 FASES DEL TRABAJO DE GRADO

El desarrollo de este trabajo se basó en tres (4) fases, que se encuentran orientadas al cumplimiento de los objetivos específicos plantados dentro del trabajo propuesto, las cuales correspondientes a:

- **Fase 1:** Revisar referentes de seguridad en computación en la nube, llevar a cabo un análisis para determinar los aspectos de seguridad que tienen en común, así como sus diferencias, con el fin de agrupar los aspectos comunes y plantear los distintos criterios de seguridad en la nube de manera objetiva.
- **Fase 2:** Analizar estándares y modelos de seguridad e identificar los aspectos relevantes con computación en la nube.
- **Fase 3:** Correlacionar de los criterios de seguridad en computación en la nube con los estándares y modelos, teniendo en cuenta los lineamientos definidos por cada uno de ellos, y evaluar el nivel de cumplimiento de los estándares teniendo como base los criterios de seguridad.
- **Fase 4:** Generar recomendaciones con base en el análisis de correlación de los criterios de seguridad con los estándares y modelos de seguridad de la información.

4.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Dentro de las herramientas utilizadas y que fueron de ayuda para el desarrollo del análisis de los criterios, estándares y modelos de seguridad de la información, para lograr generar las recomendaciones de los criterios a tener en cuenta en la seguridad en la computación en la nibe se encuentran:

- Base de datos Scopus
- Google Académico
- Buscador de Google

4.3 ALCANCES Y LIMITACIONES

Dentro del alcance del presente trabajo, se encuentra la generación de las recomendaciones respecto a la seguridad de la información en la computación de la nube, partiendo de la definición de los criterios de seguridad, continuando con la revisión del cumplimiento de dichos criterios conforme a los lineamientos definidos en los estándares y modelos de la seguridad de la información, y culminando con el respectivo análisis de la correlación para determinar el nivel de cumplimiento de los criterios en dichos estándares.

Dentro de las limitaciones encontradas para el desarrollo del trabajo se encontró, la dificultad de la adquisición de los estándares y modelos de seguridad de la información identificados dentro del análisis de la documentación. Así mismo, que la mayoría de los documentos encontrados se encontraban escritos en idioma inglés. Por lo tanto, se requirió de un esfuerzo adicional para la revisión de los documentos y análisis de los mismos.

5 PRODUCTOS A ENTREGAR

Los productos a entregar en este trabajo conforme a los objetivos planteados son:

- Lista de criterios de seguridad en la nube
- Matriz de correlación de ISO/IEC27001:2013 con los criterios establecidos.
- Matriz de correlación de ISO/IEC27017:2015 con los criterios establecidos.
- Matriz de correlación de ISO/IEC15408:2009 con los criterios establecidos.
- Matriz de correlación de Modelos con los criterios establecidos.
- Lista de recomendaciones de seguridad para computación en la nube

6 RESULTADOS OBTENIDOS

6.1 CRITERIOS DE SEGURIDAD EN LA NUBE

Cuando hablamos de seguridad en la nube nos referimos a los distintos mecanismos, técnicas y tecnologías que nos permiten resguardar la confidencialidad, integridad y disponibilidad de los datos alojada en la infraestructura de un tercero, a la cual podemos acceder y administrar mediante internet o canales dedicados. Sin embargo, la nube provee un ambiente que puede ser analizado como un todo.

Algunas fundaciones como Cloud Secutiry Alliance (CSA), normas como ISO/IEC 15408, 27001 y 270017, han abordado los problemas de la seguridad de la información, al profundizar en estos estudios se han podido identificar una serie de criterios que contienen aspectos claves que aportan a la seguridad en la nube. A continuación, se enuncian algunos de los ítems tenidos en cuenta para la definición de los criterios.

CSA describe trece criterios o aspectos de seguridad en la nube que deben ser tenidos en cuenta:

- Asuntos legales, contratos y documentos electrónicos
- Gestión de identidad, empoderamiento y acceso
- Gestión del cumplimiento y auditoria
- Gobernanza de la información
- Gobernanza y gestión de riesgos empresariales
- Plan de gestión y continuidad de negocios
- Respuesta a incidentes
- Seguridad como servicio
- Seguridad de datos y cifrado
- Seguridad en aplicaciones
- Seguridad en infraestructura

- Tecnologías relacionadas
- Virtualización y contenedores

El departamento de defensa de Estados Unidos en el documento “Cloud Security Guidance .gov Cloud Security Baseline” de 2018, aborda el tema de seguridad en la nube y destaca 30 criterios que se deben tener en cuenta las agencias de Estados Unidos cuando van a implementar servicios en la nube, los cuales se muestran a continuación.

- Administradores desconocidos
- Adquisición extranjera de CSP
- Almacenamiento extranjero de datos
- Amenaza Persistente Avanzada
- Aprovisionamiento malicioso de recursos
- Ataques basados en la web
- Bloqueo del proveedor en la nube.
- Capacidad reducida para asegurar cargas de trabajo en la nube
- Capacidad reducida para realizar pruebas forenses posteriores al evento
- Complicaciones en la gestión de parches y versiones
- Compromiso de Credenciales
- Coordinación con CSP para el cumplimiento de las leyes y reglamentos
- Corte de servicio del proveedor de la nube
- Dependencias desconocidas del CSP
- Falta de conocimiento y control sobre la cadena de suministro.
- Falta de control sobre la gestión de la seguridad física
- Fuga de memoria en la infraestructura compartida
- Incapacidad para verificar la eliminación de datos
- Información de ataque incompleta
- Mayor complejidad y carga en el personal de TI
- Mayor oportunidad de compromiso API

- Mayor potencial para amenazas internas
- Mayor potencial para la mala configuración de los servicios de seguridad.
- Modelo de negocio en la nube
- Negación de servicio
- Pérdida de conciencia situacional inducida por la latencia
- Pérdida de control sobre los datos
- Pérdida de Gobierno sobre los Activos
- Superficie de ataque aumentada debido a la tenencia múltiple
- Visibilidad y control reducidos sobre activos y operaciones de seguridad

ISO/IEC 15408 más conocido como "Common Criteria" utiliza 19 criterios para realizar la evaluación de seguridad en productos informáticos, los cuales se exponen a continuación.

- Acceso al producto
- Auditoria
- Comunicaciones
- Desarrollo
- Documentos de orientación y manuales.
- Entrega y operación
- Evaluación de vulnerabilidad
- Gestión de la configuración
- Gestión de seguridad
- Identificación y autenticación.
- Mantenimiento de aseguramiento.
- Privacidad
- Protección de datos del usuario
- Protección de las funciones de seguridad del producto.
- Pruebas
- Rutas/canales de confianza

- Soporte al ciclo de vida.
- Soporte criptográfico.
- Utilización de recursos

Con el fin de entender los aspectos de seguridad en torno a las características de seguridad Integridad, Confidencialidad, Disponibilidad, No repudio y Auditabilidad. La matriz de seguridad resultante con los aspectos y características de seguridad se encuentra adjunta en el Anexo 1 Planteamiento de criterios de seguridad en la nube

Luego de analizar las buenas practicas, se agrupan los criterios de las diferentes fuentes según sus semejanzas y como se complementen, con el fin de formular los criterios del presente trabajo, teniendo como factor diferenciador los factores de seguridad que deben ser tenidos en cuenta para implementar la seguridad en la computación en la nube. Los criterios resultantes del análisis se muestran en la Tabla 2 y son explicadas en detalle posteriormente.

Tabla 2. Criterios de seguridad y documentos de referencia.

CRITERIOS	FUENTE	ASPECTO DE SEGURIDAD
Adaptación de la organización a la nube y el recurso humano	**Department of Homeland Security, 2018**	Mayor complejidad y carga en el personal de TI
		Mayor potencial para la mala configuración de los servicios de seguridad.
	ISO/IEC 15408	Documentos de orientación y manuales.
		Entrega y operación
Cifrado y controles criptográficos	**Cloud Security Alliance, 2018**	Seguridad de datos y cifrado
	ISO/IEC 15408	Soporte criptográfico.
Continuidad del negocio, backups y flujo de información de manera segura	**Cloud Security Alliance, 2018**	Plano de gestión y continuidad de negocios
	Department of Homeland Security, 2018	Incapacidad para verificar la eliminación de datos
	ISO/IEC 15408	Soporte al ciclo de vida.
Desarrollo y aplicaciones en la nube	**Cloud Security Alliance, 2018**	Seguridad en aplicaciones
		Tecnologías relacionadas
	Department of Homeland Security, 2018	Mayor oportunidad de compromiso API
	ISO/IEC 15408	Desarrollo
		Pruebas
Geolocalización de los datos	**Department of Homeland Security, 2018**	Almacenamiento extranjero de datos
	Cloud Security Alliance, 2018	Gestión del cumplimiento y auditoria

Gestión del cumplimiento y auditoria	**ISO/IEC 15408**	Auditoria
Gobierno y gestión de activos	**Cloud Security Alliance, 2018**	Gobernanza de la información
		Gobernanza y gestión de riesgos empresariales
	Department of Homeland Security, 2018	Pérdida de control sobre los datos
		Pérdida de Gobierno sobre los Activos
		Reducción en la visibilidad y el control sobre activos y operaciones de seguridad
Leyes y normativas de la industria	**Cloud Security Alliance, 2018**	Asuntos legales, contratos y documentos electrónicos
	Department of Homeland Security, 2018	Coordinación con CSP para el cumplimiento de las leyes y reglamentos
	ISO/IEC 15408	Privacidad
Mecanismos de autenticación	**Cloud Security Alliance, 2018**	Gestión de identidad, permisos y acceso
	Department of Homeland Security, 2018	Compromiso de Credenciales
	ISO/IEC 15408	Acceso al producto
		Identificación y autenticación.
Medidas de seguridad contra hacking y malware	**Cloud Security Alliance, 2018**	Seguridad como servicio
	Department of Homeland Security, 2018	Amenaza Persistente Avanzada
		Ataques basados en la web
		Capacidad reducida para asegurar cargas de trabajo en la nube
		Complicaciones en la gestión de parches y versiones
		Negación de servicio
	ISO/IEC 15408	Comunicaciones
		Evaluación de vulnerabilidad
		Gestión de la configuración
		Gestión de seguridad
		Mantenimiento de aseguramiento.
		Protección de datos del usuario
		Protección de las funciones de seguridad del producto.
		Rutas/canales de confianza
		Utilización de recursos
Respuesta a incidentes y registros	**Cloud Security Alliance, 2018**	Respuesta a incidentes
	Department of Homeland Security, 2018	Capacidad reducida para realizar pruebas forenses posteriores al evento
		Información de ataque incompleta
		Pérdida de conciencia situacional inducida por la latencia
Riesgos asociados con el proveedor de servicios en la nube	**Cloud Security Alliance, 2018**	Virtualización y contenedores
	Department of Homeland Security, 2018	Adquisición extranjera de CSP
		Aprovisionamiento malicioso de recursos
		Bloqueo del proveedor en la nube.
		Corte de servicio del proveedor de la nube
		Fuga de memoria en la infraestructura compartida
		Modelo de negocio en la nube
		Superficie de ataque aumentada debido a la tenencia múltiple

Seguridad Física	**Cloud Security Alliance, 2018**	Seguridad en infraestructura
	Department of Homeland Security, 2018	Falta de control sobre la gestión de la seguridad física
Terceros y gestión de permisos	**Department of Homeland Security, 2018**	Administradores desconocidos
		Dependencias desconocidas del CSP
		Falta de conocimiento y control sobre la cadena de suministro.
		Mayor potencial para amenazas internas

Fuente: (Propia)

6.1.1 Adaptación de la organización a la nube y el recurso humano

En ISO/IEC 15408 se puede observar que tanto los "Documentos de orientación y manuales" como la "Entrega y operación" deben ser tenidos en cuenta para garantizar la seguridad de los productos informáticos, lo cual también aplica a las plataformas y productos utilizados por los Proveedores de Servicio en la Nube. Estos dos criterios de seguridad tienen una fuerte dependencia con el recurso humano encargado de implementar y administrar la seguridad en la nube, en la medida en que se apropien del conocimiento necesario para administrar, configurar y manipular correctamente las herramientas y productos de la nube.

El departamento de defensa de Estados Unidos en "Cloud Security Guidance .gov Cloud Security Baseline" menciona dos aspectos relacionados con el recurso humano, en la nube existe una "Mayor complejidad y carga en el personal de TI" y aumenta el riesgo de una mala configuración ya que hay "Mayor potencial para la mala configuración de los servicios de seguridad".

Al analizar los aspectos claves de la seguridad en la nube relacionados con el recurso humano se puede concluir que en adaptación de las organizaciones a la nube el recurso humano juega un papel importante, este es el responsable de generar y apropiarse del conocimiento necesario para utilizar, configurar y administrar correctamente las herramientas tecnológicas, que permiten asegurar correctamente los activos en la nube. La organización que migre servicios a la nube debe ser consciente de la carga adicional en el personal de TI, facilitar la capacitación y adaptación de este a la nube.

6.1.2 Gestión del cumplimiento y auditoria

Tanto ISO/IEC 15408 como "Security Guidance For Critical Areas of Focus in Cloud Computing v4.0" reconocen la importancia de la auditabilidad en los sistemas informáticos y como esta capacidad pude afectar el cumplimiento de políticas y normativas tanto de la industria como de gobierno a las cuales están sujetas las organizaciones. Las auditorias cobran valor al momento de evaluar el cumplimiento de las políticas organizacionales para tomar las acciones necesarias que permitan alcanzar a niveles de seguridad establecidos por la organización.

CSA en su documento "Security Guidance For Critical Areas of Focus in Cloud Computing v4.0" da como valor agregado la "gestión del cumplimiento", ya que se deben gestionar los hallazgos encontrados en las auditorias de una manera adecuada y oportuna, es así como la gestión del cumplimiento garantiza que se tomen las medidas necesarias para garantizar que se cumplan las políticas organizacionales.

Las auditorías de seguridad externas a las organizaciones con servicios en la nube y a los CSP juegan un valor importante ya que brinda objetividad a los resultados de la auditoria.

6.1.3 Continuidad del negocio, backups y flujo de información de manera segura

La continuidad de negocios es un aspecto que se analiza en "Security Guidance For Critical Areas of Focus in Cloud Computing v4.0", ISO/IEC 15408 indica que se debe dar soporte al ciclo de vida del producto y por su parte el departamento de defensa de los Estados Unidos identifica que en la nube existe una incapacidad para verificar la eliminación de datos; estos aspectos se complementan entre sí, entendiendo los activos en la nube como datos que deben ser protegidos desde su creación hasta su eliminación, en este sentido deben estar siempre disponibles y su eliminación debe ser controlada y garantizada.

La continuidad del negocio nos permite mantener los activos disponibles para que la operación no sea afectada cuando un riesgo que afecte la disponibilidad se materialice. Para

garantizar la disponibilidad las organizaciones pueden optar por utilizar backups que permitan la recuperación oportuna de los datos frente a pérdidas o para el restablecimiento de la operación en una contingencia.

La información de los backups puede contener información sensible que puede requerir un análisis más profundo, en este caso cobra importancia el flujo de información de manera segura ya que se deben implementar mecanismos que permitan que la información no sea accedida o modificada por personal no autorizado.

La nube adiciona complejidad al control del flujo de información, los backups pueden estar administrados por un tercero y sus políticas de respaldo y flujo de información pueden no tener la rigurosidad que requiere.

Se debe tener en cuenta que los datos y backups deben ser monitoreados y controlados cuando son transmitidos y eliminados ya que permanecen en los medios físicos incluso después de su eliminación; por lo tanto, los mecanismos implementados para el borrado seguro deben ser conocidos y estudiados en detalle por la organización que contrate servicios en la nube, esto permite garantizar que se implementen las políticas de seguridad de la información a cabalidad.

También se debe tener en cuenta que los productos utilizados cumplan con las características que garanticen su correcto funcionamiento y compatibilidad con tecnologías utilizadas en la nube y que permitan la migración o exportación a otras plataformas y sistemas, en este sentido cobra lugar el "soporte al ciclo de vida del producto". El software de respaldo utilizado para los datos en la nube, podría no permitir la exportación de los backups a otros proveedores o a sistemas propios, la granularidad con que se permita realizar la recuperación de los datos podría no ser la que se requiere, es decir se debe contemplar si el software permite recuperar solo unidades, carpetas o archivos, si los formatos de archivos y discos son compatibles con el software utilizado y si la exportación, transferencia y eliminación de información cumple con las políticas organizacionales.

Teniendo en cuenta lo anterior se deben tener en cuenta los "métodos de borrado seguro

utilizados por el proveedor", las "políticas de backup implementadas" y las "Políticas relacionadas a movilidad y retención de datos".

6.1.4 Geolocalización de los datos

El departamento de defensa de los Estados Unidos plantea como un aspecto a tener en cuenta la el "Almacenamiento extranjero de datos", se debe tener en cuenta que los backups mencionados en el numeral anterior también son susceptibles en este aspecto. La ubicación de los datos debe ser previamente negociada con el CSP con el fin de no incurrir en incumplimiento de la legislación que cobija a la organización con datos en la nube.

También se debe tener en cuenta la legislación en los países en los que repose físicamente la información, no todos los países cobijas los mismos derechos y deberes frente a la información y podría encontrarse que al alojar los datos en algunos países no solo se incumpla con la legislación que cobija a la organización, sino que también se pierdan derechos sobre la información en esos países, lo que podría en riesgo la confidencialidad, integridad y disponibilidad de la información.

En casos en los que se requiera realizar análisis forense y se requieran los medios físicos, podría no ser posible tener acceso a ellos o el costo para tener acceso a los mismos sea demasiado alto, a tal punto que no sea viable realizar el análisis forense del incidente informático.

6.1.5 Leyes y normativas de la industria

CSA plantea que se deben tener en cuenta "Asuntos legales, contratos y documentos electrónicos" y el departamento de defensa de Estados Unidos el cumplimiento con la legislación y normativas de la industria, se debe realizar una "Coordinación con CSP para el cumplimiento de las leyes y reglamentos", ya que es este quien tendrá la custodia de los datos en la nube y por lo tanto se debe establecer como se cumplirán con los requisitos legales y normativas de la industria.

La información confidencial como los datos privados deben ser tratados bajo controles más estrictos de seguridad, por lo tanto, la privacidad de la información cobra un valor importante en

cuanto a la legislación, la cual puede indicar bajo qué condiciones o garantías se debe almacenar, resguardar y eliminar dicha información; ISO/IEC15408 plantea la "privacidad" como uno de los aspectos a tener en cuenta en el producto y esta característica debe estar implementada en aplicaciones que se utilicen en la nube.

6.1.6 Gobierno y gestión de activos

El gobierno de los datos es un factor importante a tener en cuenta cuando se utilizan tecnologías de computación en la nube. En la nube existen factores adicionales que deben ser tenidos en cuenta para garantizar la gobernanza de los datos, los datos se encuentran ubicados en la infraestructura del CSP, hecho que implica una responsabilidad compartida que debe ser abordada desde el ámbito contractual y mediante controles internos.

Cuando un tercero tiene algún nivel de control sobre los datos, se puede perder visibilidad en algún momento de su ciclo de vida, lo que implica una pérdida de gobernanza, es por esto que las políticas organizacionales deben ser ajustadas para cobijar los datos en la nube.

CSA propone abordar la gobernanza de datos en la nube mediante una perspectiva de riesgos, esto permite alinear los controles y políticas con los objetivos del negocio. De esta manera se logra concentrar los esfuerzos y recursos en donde tienen un aporte más valioso para la organización.

El ministerio de defensa de Estados Unidos identifica dos riesgos asociados con la gobernanza "Pérdida de Gobierno sobre los Activos" y "Reducción en la visibilidad y el control sobre activos y operaciones de seguridad". CSA aborda este criterio en "Gobernanza de la información" planteando una comprensión del ciclo de vida de los datos los diferentes escenarios y como la "Gobernanza y gestión de riesgos empresariales" nos ayudan a asegurarlos en todo el ciclo de vida.

6.1.7 Mecanismos de autenticación

Los mecanismos de autenticación son abordados por CSA en la “Gestión de identidad, permisos y acceso”, ISO/IEC 15408 evalúa el “Acceso al producto” y la “Identificación y autenticación”, mientras que el departamento de defensa de los Estados Unidos desde una perspectiva de riesgos analiza el “Compromiso de Credenciales” en computación en la nube.

Estos mecanismos deben ser monitoreados, auditados y gestionados correctamente, el análisis de registros o la detección automática de anomalías en el uso de credenciales pueden ayudar a mantener seguras las credenciales.

También se deben minimizar las credenciales de administración con permisos elevados y utilizar perfiles para establecer limitaciones en el uso de las mismas.

El múltiple factor de autenticación es uno de los mecanismos más efectivos para asegurar las credenciales en la nube y por lo tanto debe ser utilizado siempre que sea posible.

6.1.8 Medidas de seguridad contra hacking y malware

ISO/IEC 15408 aborda la seguridad contra malware teniendo como perspectiva el desarrollo seguro de aplicaciones asegurando las comunicaciones y canales de confianza, evaluando las vulnerabilidades, gestionando la configuración y seguridad de manera adecuada y manteniendo este aseguramiento para proteger los datos del usuario.

El departamento de defensa de Estados Unidos identifica que pueden existir “complicaciones en la gestión de parches y versiones” por lo tanto se debe monitorear y supervisar la instalación de parches y actualizaciones.

Las APTs, ataques basados en web y negación de servicios son un riesgo latente en la nube, por lo tanto, las organizaciones deben trabajar junto con los CSP para adoptar medidas de seguridad basadas en defensa en profundidad. Aquí entran en juego configuraciones a nivel de firewall, sistemas de detección y prevención de intrusos (IDPS), y otros dispositivos y herramientas que permitan asegurar el perímetro, identificar y neutralizar las amenazas.

El análisis de vulnerabilidades permite prever y corregir las debilidades que un hacker podría utilizar para afectar la seguridad de los servicios en la nube.

CSA evalúa las ventajas que ofrece la seguridad como servicio, su integración con las APIs del proveedor y otras funcionalidades que pueden ser de interés para asegurar ambientes en la nube.

6.1.9 Riesgos asociados con el proveedor de servicios en la nube

Cuando los activos de una organización son migrados a la nube y pasan a ser custodiados por el proveedor de servicios en la nube, aparecen nuevos riesgos relacionados con el proveedor de servicios y con las tecnologías que utiliza para ofrecer sus servicios, es decir la virtualización.

Las tecnologías de virtualización deben ser aseguradas correctamente ya que ellas gestionan los sistemas virtualizados y cualquier incidente de seguridad podría afectar la integridad disponibilidad y confidencialidad de los equipos huéspedes. La tenencia múltiple implica que un usuario en una máquina virtual podría salir (escapar) de ella y tener acceso a otras máquinas virtuales que se encuentren hospedadas en el mismo servidor físico, lo que supone una mayor superficie de ataque cuando se logran evadir las medidas de seguridad del CSP para aislar las máquinas virtuales.

El monitoreo del tráfico y otros mecanismos de control se comportan diferente y deben ser ajustados para su trabajo en la nube, teniendo en cuenta que el tráfico entre máquinas virtuales no necesariamente pasara a través controles como un firewall o un correlacionador de eventos, etc. Estos aspectos son estudiados en detalle por CSA, sin embargo, el departamento de defensa de los estados unidos tiene en cuenta “Fuga de memoria en la infraestructura compartida” y “Superficie de ataque aumentada debido a la tenencia múltiple”, ya que no se pueden controlar exactamente donde se procesarán los datos y los recursos son compartidos, por lo tanto, podría presentar un acceso no autorizado.

El departamento de defensa de los Estados Unidos centra su atención en riesgos relacionados con el proveedor de servicios en la nube como la “Adquisición extranjera de CSP”, “Bloqueo del proveedor en la nube”, “Corte de servicio del proveedor de la nube” y cambios en el “Modelo de negocio” del CSP, estos causarían indisponibilidad de los servicios en la nube y afectarían los activos si no se tienen en cuenta planes de contingencia.

6.1.10 Respuesta a incidentes y registros

Los registros de evento, el monitoreo continuo y el plan de respuesta a incidentes juegan un papel importante para identificar a los responsables del incidente. El plan debe contener las responsabilidades y el papel que juegan las partes cuando un incidente ocurre con el fin de garantizar la cadena de custodia y culminar el plan de respuesta a incidentes a cabalidad.

Cuando un incidente ocurre en la nube existe una latencia durante la cual se ejecutan los procedimientos establecido por el proveedor para comunicar el incidente a sus clientes, adicionalmente los reportes pueden estar incompletos, por estos motivos cobra importancia que los clientes monitoreen los servicios en la nube y guarden registro de los eventos en un lugar que pueda ser consultado cuando un incidente ocurra.

El registro de los eventos no ocurre en tiempo real, existe un tiempo desde que los eventos ocurren, hasta que son almacenados en el registro con la información y categorización. Estos tiempos aumentan dependiendo de la cantidad de datos que deben ser procesados y en la nube estos tiempos pueden ser considerables por la cantidad de conexiones que debe manejar el proveedor.

6.1.11 Seguridad física

La seguridad física cuando se contratan servicios en la nube es asumida por el proveedor contratado para el servicio, por este motivo se deben conocer las políticas y controles de acceso físico que este implementa para garantizar que estén alineados con las políticas internas de la organización.

Las organizaciones deben verificar periódicamente que los CSPs cumplan con las buenas prácticas y regulaciones de la infraestructura física.

Las cargas de trabajo a las que son sometidos los equipos físicos puede ocasionar lentitud, bloqueos y cuellos de botella cuando sobrepasan sus capacidades, por este motivo se deben conocer las limitaciones y capacidades, para que los administradores puedan configurarlas correctamente.

6.1.12 Terceros y gestión de permisos

Cuando se contratan servicios en la nube el proveedor puede hacer uso de terceros para realizar algunas funciones relacionadas con los servicios en la nube, esto adiciona una brecha de seguridad ya que pueden existir "Administradores desconocidos", "Dependencias desconocidas del CSP", "Falta de conocimiento y control sobre la cadena de suministro" y hay un "Mayor potencial para amenazas internas".

Los terceros deben cumplir con las políticas de seguridad y deben ser de conocimiento de organización que contrate servicios en la nube, de lo contrario pueden representar un vector de ataque desconocido y los riesgos asociados al tercero no serán analizados ni tratados.

El personal empleado por terceros puede tener acceso privilegiado para realizar sus funciones, sin embargo, deben contar con el conocimiento requerido para realizar sus tareas correctamente y son un factor por el que puede manipularse información que ponga en riesgo la seguridad de los activos de las organizaciones con servicios en la nube. Por este motivo las organizaciones deben trabajar en conjunto con el CSP para detectar y mitigar estas amenazas.

6.1.13 Desarrollo y aplicaciones en la nube

Cuando se desarrolla software para la nube o se utiliza software en la nube se den considerar cual es el sipo de servicio más adecuado para ejecutar dicho software, también es importante

garantizar que los aspectos de diseño, arquitectura, desarrollo y el ciclo de vida sean abordados desde la perspectiva de seguridad.

Las tecnologías como internet de las cosas, big data y otras tecnologías emergentes adicionan nuevos retos de seguridad que deben ser tenidos en cuenta cuando se desarrollan aplicaciones en la nube.

Debido a que en la nube se utilizan APIs para gestionar los activos en la nube, estas deben ser desarrolladas, validadas, probadas y monitoreadas para puedan ser utilizadas de manera segura y no pongan en riesgo los activos que las utilizan.

ISO/IEC 15408 evalúa el desarrollo y pruebas de las aplicaciones y APIs para que no sean un riesgo de seguridad.

6.1.14 Cifrado y controles criptográficos

El cifrado y almacenamiento de los datos deben ser analizado para que la información no sea accedida por personal no autorizado, los backups también deben hacer uso de llaves de cifrado ya que pueden contener grandes cantidades de información, se deben utilizar claves gestionadas por el cliente de ser posible y no utilizar las mismas claves para todos los activos. Para lograr un adecuado uso de las técnicas de cifrado y gestión de clave se deben tener en cuenta las normas NIST SP-800-57, ANSI X9.69 y ANSI X9.73.

6.2 Correlación de Criterios de Seguridad con Estándares y Modelos

A continuación, se realiza una revisión de los estándares ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 15408 con el fin de identificar cuáles de los criterios de seguridad propuestos son tenidos en cuenta por dichos estándares. En los dos primeros estándares se califica el cumplimiento de cada uno de los controles con los criterios definidos en el numeral 6.1, de esta manera se puede llegar a dar recomendaciones relacionadas con los estándares y criterios. Los modelos también son

correlacionados con los criterios definidos en el numeral anterior.

6.2.1 ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información

Se llevó a cabo el análisis de los lineamientos definidos por este estándar ISO 27001:2013 con el fin de validar el posible cumplimiento de los criterios de seguridad definidos para la computación en la nube. A continuación, se enuncian los controles de la norma relacionados con los criterios de seguridad para posteriormente analizar su cumplimiento con los criterios establecidos.

6.1- Acciones para tratar riesgos y oportunidades. El requisito define que la organización debe determinar los riesgos y oportunidades que deban tratarse según el análisis del contexto, teniendo en cuenta los procesos de análisis, valoración y tratamiento de los mismos.

A.6.1.1- Roles y Responsabilidad de Seguridad de la Información. En el Anexo indica que se debe definir y asignar todas las responsabilidades de la seguridad de la información.

A.7.2.2- Conciencia, educación y entrenamiento de Seguridad de la Información. Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo."

A.8.1.1- Inventario de activos. Se deben identificar los activos asociadas con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

A.8.1.2- Propiedad de activos. Los activos mantenidos en el inventario deben tener un propietario.

A.8.1.3- Uso aceptable de los activos. Se deben identificar documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalación de procedimientos de información.

A.8.1.4- Devolución de activos. Todos los empleados y usuarios de partes deben devolver todos los activos de la organización que se encuentren a su cargo al terminar su empleo, contrato o acuerdo.

A.9.2.1- Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

A.9.2.2- Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios y para todos los sistemas y servicios.

A.9.2.3- Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

A.9.2.4- Gestión de información de autenticación secreta. La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.

A.9.2.5- Revisión de los derechos de acceso de usuarios. Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares

A.9.2.6- Retiro y ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

A.10- Criptografía. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información, además, se requiere desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

A.11.1.1- Perímetro de seguridad físico. Se deben definir y usar perímetros de seguridad y usarlos para proteger áreas que contengan información confidencial o critica en instalaciones de manejo de información.

A.11.1.2- Controles físicos de entrada. Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.

A.11.1.3- Seguridad de oficinas, recintos e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

A.11.1.4. Protección contra amenazas externas y del ambiente. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

A.11.1.5- Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

A.12.2.1- Controles contra software malicioso. Se debe implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de los usuarios, para proteger contra código maliciosos.

A.12.4.1- Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros y eventos de seguridad de la información.

A.12.4.2- Protección de la información y registros. Los registros deben ser protegidos

contra alteración y acceso no autorizado.

A.12.4.3- Registros de administrador y operador. Las actividades de administrador y operador deben ser registradas, y estos deben ser protegidos y revisados con regularidad.

A.12.4.4- Sincronización de relojes. Todos los relojes de la organización deben estar sincronizados con una misma fuente de tiempo.

A.12.6.1- Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

A.14.2.1- Política de desarrollo seguro. Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.

14.2.2- Procedimientos de control de cambios. Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios

14.2.3- Revisión técnica de aplicaciones después de cambios a la plataforma operativa. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización

14.2.4- Restricción de cambios a paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.

14.2.5- Principios de construcción de los sistemas seguros. Se deben establecer,

documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

14.2.6- Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

14.2.7- Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

14.2.8- Pruebas de seguridad del sistema. Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.

14.2.9- Pruebas de aceptación del sistema. Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.

A.14.3.1- Protección de datos de prueba. Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.

A.15.1.1- Política de Seguridad de la Información para relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociadas con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.

A.15.1.2- Atención de tópicos de seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de Tl para la información de la organización.

A.15.1.3- Cadena de suministros de TIC. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociadas con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

A.16.1.1- Responsabilidades y Procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

A.16.1.2- Reporte de eventos de Seguridad de la Información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

A.16.1.3- Reporte de debilidades de Seguridad de la Información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

A.16.1.4- Valoración y decisión de eventos de Seguridad de la Información. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

A.16.1.5- Respuesta a incidentes de Seguridad de la Información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

A.16.1.6- Aprendizaje de incidentes de Seguridad de la Información. El conocimiento adquirido al analizar y observar incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7- Recolección de evidencia. La organización debe definir y aplicar procedimientos

para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

A.17.1.1- Planeación de la continuidad de la seguridad de la información. Planeación de la continuidad de la seguridad de la información.

A.17.1.2- Implementación de la continuidad de la seguridad de la Información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

A.17.1.3- Verificación, revisión y evaluación de continuidad de la seguridad de la Información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

A.18.1.1- Identificación de la legislación aplicable y de los requisitos contractuales. Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.

A.18.1.4- Privacidad y protección de información de datos personales. Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

A.18.2.1- El enfoque de La organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

A.18.2.2- El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

A.18.2.3- Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

6.2.1.1 Matriz de correlación de ISO/IEC 27001 y criterios de seguridad

Los criterios permiten evaluar el cumplimiento del estándar con cada uno de ellos, con este fin son correlacionados con los lineamientos definidos en los estándares ISO/IEC 27001. La tabla 3 muestra la correlación de los criterios con los controles y requisitos de la norma, los cuales son evaluados según su nivel de cumplimiento, se establecen tres niveles para medir el cumplimiento que puede ser Bajo (B), Medio (M) y Alto (A) según los aspectos que tiene en cuenta la norma para cumplir con los criterios establecidos, la tabla se muestra a continuación.

Tabla 3. Matriz de correlación de ISO/IEC 27001:2013 y criterios de seguridad, y nivel de cumplimiento del estándar con los criterios.

CRITERIO	ISO/IEC27001	NIVEL DE CUMPLIMIENTO
6.1.1. Adaptación de la organización a la nube y el recurso humano	A.6.1.1- Roles y Responsabilidad de Seguridad de la Información A.7.2.2- Conciencia, educación y entrenamiento de Seguridad de la Información	A
6.1.2. Gestión del cumplimiento y auditoría	A.18.2- Cumplimiento con Requerimientos Legales y Contractuales	A
6.1.3. Continuidad del negocio, backups y flujo de información de manera segura	A.17.1- Seguridad de la Información en la Continuidad	A
6.1.4. Geolocalización de los datos	NO INCLUIDO	B
6.1.5. Leyes y normativas de la industria	A.18.1.1- Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.4- Privacidad y protección de información de datos personales	B

6.1.6. Gobierno y gestión de activos	A.8.1- Responsabilidad de los Activos A.15.1.1- Política de Seguridad de la Información para relaciones con proveedores. A.15.1.2- Atención de tópicos de seguridad dentro de los acuerdos con proveedores.	A
6.1.7. Mecanismos de autenticación	A.9.2- Gestión de Accesos de Usuario	A
6.1.8. Medidas de seguridad contra hacking y malware	A.12.2.1- Controles contra software malicioso A.12.6.1- Gestión de vulnerabilidades técnicas.	A
6.1.9. Riesgos asociados con el proveedor de servicios en la nube	6.1- Acciones para tratar riesgos y oportunidades	B
6.1.10. Respuesta a incidentes y registros	A. 16.1- Gestión de Incidentes de Seguridad de la Información y Mejoras A.12.4- Registros y seguimiento	A
6.1.11. Seguridad Física	A.11.1- Áreas Seguras	A
6.1.12. Terceros y gestión de permisos	A.15- Relaciones con Proveedores	M
6.1.13. Desarrollo y aplicaciones en la nube	A.14- Adquisición, Desarrollo y Mantenimiento de Sistemas	A
6.1.14. Cifrado y controles criptográficos	A.10- Criptografía.	A

Fuente: (Propia)

6.2.2 ISO/IEC 27017:2015 Código de práctica para los controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube

A continuación, se enuncian y describen las definiciones y controles de ISO/IEC 27017 teniendo en cuenta su relevancia para la seguridad de la información en servicios en la nube, con el fin de poder analizar su cumplimiento con los criterios y desarrollar la matriz de cumplimiento.

4.4- Evaluación de riesgos de seguridad de la información en servicios en la nube. Los requerimientos de seguridad de la información son identificados por los riesgos de seguridad de la información. Cada cliente o proveedor de servicios en la nube debe completar su propia información de evaluación de riesgos de seguridad de la información para determinar el impacto a su negocio en relación a la probabilidad de vulnerar la seguridad de la información o falla de los controles.

5.1- Gestión de la alta dirección para seguridad de la información. Las organizaciones deben contar con una política de seguridad de la información en la nube acorde a los riesgos organizacionales y se deben tener en cuenta los niveles de seguridad ofrecidos por el proveedor de servicios en la nube. Adicionalmente se deben revisar las políticas de seguridad de la información.

6.1.1- Roles y responsabilidades de seguridad de la información. La división de las responsabilidades de seguridad de la información entre el cliente del servicio en la nube y el proveedor del servicio en la nube debe estar claramente definida y documentada.

7- Seguridad de los recursos humanos. En este numeral se establecen teniendo en la ISO 27002 los controles asociados al personal; Antes del empleo; Selección; Términos y condiciones del empleo; Durante el empleo; Responsabilidades de la Gerencia; Conciencia, educación y capacitación sobre la seguridad de la información; Proceso disciplinario; Terminación y cambio de empleo y; Terminación o cambio de responsabilidades del empleo.

8- Gestión de Activos. Para los lineamientos de la gestión de activos e información, se establece como recomendación lo establecido en la ISO 27002 con respecto a: Responsabilidad por los activos; Inventario de activos (Los tipos de activos del cliente del servicio en la nube pueden variar dependiendo del servicio. El software utilizado para la provisión de SaaS puede ser un activo del cliente del servicio en la nube para el proveedor de SaaS en relación con IaaS como su infraestructura); Propiedad de los activos, Uso aceptable de los activos; Retorno de activos; Clasificación de la información; Etiquetado de la información; Manejo de Activos; Manejo de Medios; Gestión de medios removibles; Eliminación de medios y; Transferencia de medios físicos.

9 Control de Acceso. Dentro de este ítem la norma trata a cerca de controles relacionados a: Requisitos de la empresa para el control de acceso; Política de control de acceso; Acceso a la red y servicios de red; Gestión de acceso de usuarios; Registro y baja de usuarios; Aprovisionamiento de acceso a usuarios; Gestión de derechos de acceso privilegiado; Gestión de información de autenticación secreta de usuarios; Revisión de los derechos de acceso de usuarios, Retiro o ajuste de derechos de acceso; Responsabilidades de los usuarios; Uso de la información

de autenticación secreta; Control de acceso al sistema y aplicación; Restricción de acceso a la información y; Sistema de gestión de contraseñas.

9.4.5- Control de acceso al código fuente de los programas. En este numeral se determina el control relacionado con el acceso al código fuente basado en la ISO 27002.

10- Criptografía. En este numeral se describen los controles con base en la norma ISO 27002 correspondientes a: Controles criptográficos, Política sobre el uso de controles criptográficos (en donde el proveedor debe confirmar las funcionalidades de la criptografía proporcionadas en el servicio son adecuadas con las políticas definidas en la organización); Gestión de claves (se deben identificar las claves criptográficas que se debe administrar en el servicio en la nube y establecer el procedimiento para la administración de dichas claves. Es importante tener en cuenta que el cliente del servicio en la nube no debe permitir que el proveedor almacena y administre las claves de cifrado a nombre del cliente).

11- Seguridad física y ambiental. Dentro de los controles definidos en este ítem se encuentran los controles de la ISO 27002 correspondientes a: Perímetro de seguridad física (el cliente debe solicitar información sobre el perímetro de seguridad física para confirmar que las especificaciones satisfacen sus requisitos); Controles de ingreso físico; Asegurar oficinas, áreas e instalaciones; Protección contra amenazas externas y ambientales; Trabajo en áreas seguras; Área de despacho y cargo; Ubicación y protección de los equipos; Servicios e suministro; Seguridad en el cableado; Mantenimiento de equipos; Retiro de activos; Seguridad de equipos y activos fuera de las instalaciones; Disposición y utilización segura de equipos; Equipos de usuario desatendido; Política de escritorio y pantalla limpia.

12.1.2.- Gestión del Cambio. Dentro de este control se propone, que el cliente del servicio en la nube debe gestionar los cambios que realice el proveedor dentro del proceso de gestión de cambios del cliente, en donde se determinen las fechas y horarios, los cambios a ejecutar, así como una alerta de inicio y finalización del cambio.

12.1.3- Gestión de la capacidad. El cliente del servicio en la nube puede considerar lo

siguiente en la gestión de la capacidad si le fue entregada por el proveedor del servicio: a) entorno del sistema:

a) entorno del sistema:

1) Capacidad de almacenamiento de datos;

2) Capacidad de las redes y equipos, incluida la red virtual en el entorno del servicio en la nube (por ejemplo, ancho de banda, número máximo de sesiones);

3) Rendimiento del sistema esperado o acordado;

4) Tiempo de entrega para tener capacidad adicional o rendimiento del sistema, y unidad mínima de entrega;

5) Capacidad máxima y rendimiento del sistema;

6) Redundancia y diversidad de sistemas

7) Redundancia y diversidad de accesos a la red.

b) estadísticas sobre el uso de recursos del sistema:

1) estadísticas en un período de tiempo dado;

2) uso máximo de recursos del sistema.

12.1.4- Separación de los entornos de desarrollo, pruebas y operaciones. Los controles asociados a la separación de los entornos de desarrollo, prueba y producción, conforme a lo planteado en la ISO 27002, se debe tener en cuenta, que dichos ambientes deben encontrarse separados, con el fin de proteger la información y que se lleven a cabo las pruebas necesarias para poner en producción los servicios, sistemas, aplicaciones, etc.

12.2- Protección contra software malicioso (malware). Este control determina que se debe tener en cuenta las buenas prácticas definidas por la ISO 27002, en donde se describe: Controles contra software malicioso.

12.3- Respaldo. En este control como en ítems anteriores, se plantea como buena práctica tener en cuenta lo establecido en la ISO 27002 con respecto a: Respaldo de la información (en donde se debe definir una política y procedimiento definiendo las responsabilidades de parte del proveedor respecto al respaldo, la restauración, seguridad de las copias de seguridad y periodos de retención de los datos).

12.4- Registros y monitoreo. Dentro de los controles establecidos se encuentra: Registro de eventos (se debe establecer claramente procedimientos para desarrollar actividades del monitoreo acerca del uso de los servicios en la nube); Protección de información de registros; Registros de administrador y del operador, Sincronización de reloj.

12.5- Control del software operacional. Dentro de este ítem se determina las responsabilidades del proveedor con respecto al control del software operacional; Instalación de software en los sistemas operacionales respecto a: seguimiento, registros de supervisión del software en ejecución.

12.6- Gestión de vulnerabilidad técnica. Adicional a lo indicado con respecto a la ISO 27002, este estándar recomienda, la inclusión de la gestión de vulnerabilidades en el servicio en donde se especifique la forma de identificar las vulnerabilidades, política de respuesta a las vulnerabilidades y el acuerdo de aceptación de las vulnerabilidades.

12.7- Consideraciones para la auditoría de los sistemas de información. Dentro de las indicaciones brindadas en el estándar, se considera con respecto a este control, los controles de auditoría para los sistemas de información conforme a lo indicado en la ISO 27002.

13- Seguridad de las comunicaciones. Dentro de este control se establece lo relacionado con: Gestión de la seguridad en la red; Controles de la red; Seguridad servicios de seguridad; Controles de la red; Seguridad de servicios de red (se debe solicitar al proveedor las especificaciones relacionadas con la seguridad en las redes, incluida la capacidad de red y redundancia); Segregación en redes (validar especificaciones funcionales sobre la división de las redes en dominios separados y segregación con respecto a otras empresas que estén en la misma red); Transferencia de información; Políticas y procedimientos de transferencia de información; Acuerdo sobre transferencia de información; Mensajes electrónicos; Acuerdos de confidencialidad o no divulgación.

14- Adquisición, desarrollo y mantenimiento de sistemas. Dentro de este ítem se habla de

controles asociados a: Análisis y especificación de requisitos de seguridad de la información (especificando los requisitos de seguridad en el servicio de la nube, riesgos específicos); Aseguramiento de servicios de aplicaciones sobre redes públicas; Protección de transacciones en servicios en aplicación; seguridad en los procesos de desarrollo y soporte; Política de desarrollo seguro; Procedimiento de control de cambio del sistema; Revisión técnica de aplicaciones después de cambios a la plataforma; Restricción sobre cambios a los paquetes de software; Principio de ingeniería de sistemas seguros; Ambiente de desarrollo seguro; desarrollo contratado externamente; Pruebas de seguridad del sistema; Pruebas de aceptación del sistema y; Protección de datos de prueba.

15- Relación con los proveedores. En este ítem se encuentran los lineamientos para contratar proveedores de servicios en la nube, dentro de los controles propuestos y alineados con la ISO 27002 se encuentran: Seguridad en las relaciones con los proveedores, Política de seguridad de la información para las relaciones con los proveedores (revisar cuando el proveedor utiliza servicios en la nube de otro proveedor, es importante validar que por lo menos que las obligaciones de seguridad coincidan al menos con los requisitos de seguridad pactados entre el cliente y el proveedor); Abordar la seguridad dentro de los acuerdos con proveedores (se propone que el proveedor tenga en cuenta al memento de suministrar el servicio en la nube, los acuerdos pactados, las políticas definidas y la revisión de riesgos tanto con el cliente, como con sus mismos proveedores, así mismo, se pueden establecer controles asociados con el recurso humano); Cadena de suministro de tecnología de información y comunicaciones (el proveedor debe garantizar que los niveles de servicios subcontratados, no interfieran los niveles de servicios acordados con sus clientes); Gestión de entrega de servicios del proveedor; Monitoreo y revisión de los servicios del proveedor; Gestión del cambio a los servicios del proveedor.

16.- Gestión de incidentes de seguridad de la información. Este parametro establece los controles conforme a la ISO 27002 contemplando los siguientes controles: Gestión de incidentes de seguridad de la información y mejoras; Responsabilidades y procedimientos (el cliente debe verificar el proceso de comunicación al presentarse incidentes graves en el proveedor); Reporte de eventos de seguridad de la información; Reporte de debilidades de seguridad de la información; Evaluación y decisión sobre eventos de seguridad de la información (es importante evaluar los

lineamientos definidos por el proveedor y revisar el marco de la gestión de incidentes cuando sea necesario); Respuesta a incidentes de seguridad de la información; Aprendizaje de los incidentes de seguridad de la información; Recolección de evidencia (El cliente debe identificar la información que pueda servir como evidencia en el servicio de la nube, establecer los procedimientos en los cuales se pueda adquirir la información, garantizar que la evidencia se preserve dentro de la duración del servicio).

17- Aspectos de la seguridad de la información en la continuidad del negocio. Dentro de los controles establecidos dentro de este numeral se encuentran: Continuidad de seguridad de la información; Planificación de continuidad de seguridad de la información, Implementación de la continuidad de la seguridad de la información; Verificación, revisión y evaluación de la continuidad de seguridad de la información, redundancia, Disponibilidad de instalaciones de procesamiento de información.

18.1.- Cumplimiento con requisitos legales y contractuales. Los controles propuestos dentro de este ítem, conforma a lo establecido en el estándar se encuentran: Identificación de los requisitos contractuales y de legislación aplicable (El cliente debe determinar los requisitos legales y contractuales nacionales y extranjeros según el uso de los servicios en la nube); Derechos de propiedad intelectual; Protección de registros; Privacidad y protección de datos personales (El cliente debe identificar los requisitos legales, normativos y contractuales nacionales y extranjeros de la protección de datos y la privacidad de la información conforme al propósito del uso del servicio en la nube); Regulación de controles criptográficos (El cliente debe solicitar al proveedor verificar la tecnología criptográfica utilizada no estén en conflicto con regulaciones en los países o regiones que prestan el servicio).

18.2.- Revisiones de seguridad de la información. En este ítem se indican controles tales como: Revisión independiente de la seguridad de la información; Cumplimiento de políticas y normas de seguridad (los proveedores deben asegurar procedimientos para cumplir con los acuerdos de nivel de servicio); Revisión de cumplimiento técnico (El cliente debe confirmar la información para la verificación del cumplimiento técnico para la prestación de servicio en la nube).

CDL.6.3.- Relación entre el cliente y el proveedor del servicio en la nube. Se debe establecer y mantener una relación colaborativa entre el cliente y el proveedor del servicio en la nube pera la gestión de la seguridad de la información, incluyendo: Declaración de responsabilidad; Sistema de intercambio de información.

6.2.2.1 Matriz de correlación de ISO/IEC 27017 y criterios de seguridad

Los criterios permiten evaluar el cumplimiento del estándar con cada uno de ellos, con este fin son correlacionados con los lineamientos definidos en los estándares ISO/IEC 27017. La tabla 4 muestra la correlación de los criterios con los controles y requisitos de la norma, los cuales son evaluados según su nivel de cumplimiento, se establecen tres niveles para medir el cumplimiento que puede ser Bajo (B), Medio (M) y Alto (A) según los aspectos que tiene en cuenta la norma para cumplir con los criterios establecidos, la tabla se muestra a continuación.

Tabla 4. Matriz de correlación de ISO/IEC 27017 y criterios de seguridad, y nivel de cumplimiento del estándar con los criterios.

CRITERIO	ISO/IEC 27017	NIVEL DE CUMPLIMIENTO
6.1.1. Adaptación de la organización a la nube y el recurso humano	7- Seguridad de los recursos humanos	A
6.1.2. Gestión del cumplimiento y auditoría	12.7- Consideraciones para la auditoría de los sistemas de información 18.2.- Revisiones de seguridad de la información	A
6.1.3. Continuidad del negocio, backups y flujo de información de manera segura	12.3- Respaldo 17- Aspectos de la seguridad de la información en la continuidad del negocio	A
6.1.4. Geolocalización de los datos	NO INCLUIDO	B
6.1.5. Leyes y normativas de la industria	18.1.- Cumplimiento con requisitos legales y contractuales	M
6.1.6. Gobierno y gestión de activos	5.1- Gestión de la alta dirección para la seguridad de la información. 8- Gestión de Activos	A
6.1.7. Mecanismos de autenticación	9- Control de Acceso	A
6.1.8. Medidas de seguridad contra hacking y malware	12.2- Protección contra software malicioso (malware) 12.6- Gestión de vulnerabilidad técnica	A
6.1.9. Riesgos asociados con el proveedor de servicios en la nube	4.4- Evaluación de riesgos de seguridad de la información en servicios en la nube.	M
6.1.10. Respuesta a incidentes y registros	12.4- Registros y monitoreo 16- Gestión de incidentes de seguridad de la información	A

6.1.11. Seguridad Física	11- Seguridad física y ambiental 12.1.2- Gestión del cambio 12.1.3- Gestión de la capacidad 13- Seguridad de las comunicaciones	A
6.1.12. Terceros y gestión de permisos	6.1.1- Roles y responsabilidades de seguridad de la información 12.5- Control del software operacional 15- Relación con proveedores CDL.6.3.- Relación entre el cliente y el proveedor del servicio en la nube	A
6.1.13. Desarrollo y aplicaciones en la nube	9.4.5- Control de acceso al código fuente de los programas 12.1.4- Separación de los entornos de desarrollo, pruebas y operaciones 14- Adquisición, desarrollo y mantenimiento de sistemas	A
6.1.14. Cifrado y controles criptográficos	10- Criptografía	A

Fuente: (propia)

6.2.3 Matriz de correlación de ISO/IEC 15408:2009 y criterios de seguridad

ISO/IEC 15408 está orientado a la evaluación de productos o aplicativos, sin embargo, los servicios en la nube permiten desarrollar e implementar aplicaciones por lo que su uso permite asegurar los productos utilizados en la nube para que cumplan con los niveles de seguridad deseados. La tabla 5 muestra la correlación de los criterios de seguridad definidos con el estándar ISO/IEC 15408.

Tabla 5. Matriz de correlación de ISO/IEC15408:2009 con los criterios establecidos

CRITERIO	ISO15408
6.1.1. Adaptación de la organización a la nube y el recurso humano	Documentos de orientación y manuales. Entrega y operación
6.1.2. Gestión del cumplimiento y auditoría	Auditoría
6.1.3. Continuidad del negocio, backups y flujo de información de manera segura	Soporte al ciclo de vida.
6.1.4. Geolocalización de los datos	NO INCLUIDO
6.1.5. Leyes y normativas de la industria	Privacidad
6.1.6. Gobierno y gestión de activos	NO INCLUIDO
6.1.7. Mecanismos de autenticación	Acceso al producto Identificación y autenticación.

6.1.8. Medidas de seguridad contra hacking y malware	Comunicaciones Evaluación de vulnerabilidad Gestión de la configuración Gestión de seguridad Mantenimiento de aseguramiento. Protección de datos del usuario Protección de las funciones de seguridad del producto. Rutas/canales de confianza Utilización de recursos
6.1.9. Riesgos asociados con el proveedor de servicios en la nube	NO INCLUIDO
6.1.10. Respuesta a incidentes y registros	NO INCLUIDO
6.1.11. Seguridad Física	NO INCLUIDO
6.1.12. Terceros y gestión de permisos	NO INCLUIDO
6.1.13. Desarrollo y aplicaciones en la nube	Desarrollo Pruebas
6.1.14. Cifrado y controles criptográficos	Soporte criptográfico.

Fuente: (propia)

6.2.4 Matriz de correlación de modelos y criterios de seguridad

Los modelos descritos en el capítulo 2.2.2 son utilizados por algunos de los criterios definidos, para identificar en que criterios pueden ser empleados los modelos se realiza la matriz de correlación de modelos y criterios de seguridad. La tabla 6 muestra la correlación de los criterios con los modelos.

Tabla 6. Matriz de correlación de Modelos y criterios de seguridad.

MODELOS	CRITERIOS DE SEGURIDAD EN LA NUBE													
	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5	6.1.6	6.1.7	6.1.8	6.1.9	6.1.10	6.1.11	6.1.12	6.1.13	6.1.14
Máquinas de estado	-	-	-	-	-	-	-	X	-	-	-	-	X	-
Bell-LaPadula	-	-	X	-	-	-	X	X	-	-	-	-	X	-
Biba	-	-	X	-	-	-	X	X	-	-	-	-	X	-
Clark-Wilson	-	-	X	-	-	-	X	X	-	-	-	-	X	-
Flujo de información	-	-	X	-	-	-	-	X	-	-	X	-	X	X
No interferencia	-	-	X	-	-	-	X	X	-	-	-	-	X	X
Lattice	-	-	X	-	-	-	X	X	-	-	-	-	X	-
Brewer and Nash	-	-	X	-	-	-	-	X	-	-	X	-	X	-

Graham-Denning	-	-	-	-	-	-	X	X	-	-	-	-	X	-
Harrison-Ruzzo-Ullman	-	-	-	-	-	-	X	-	-	-	-	-	X	-

Fuente: (propia)

6.3 Recomendaciones

En los numerales 6.2.1 y 6.2.2 se calificó el cumplimiento de los controles contemplados por ISO/IEC 27001 e ISO/IEC 27017 con los criterios, de esta manera en este numeral se presentan recomendaciones relacionadas con estos estándares y criterios. Del mismo modo después de llevar a cabo la revisión y análisis del estándar ISO/IEC15408:2009, los modelos y las buenas prácticas de la industria se proponen las siguientes recomendaciones:

- Se debe tener claridad sobre el tipo de servicio que se desea contratar en la nube, ya que SaaS, PaaS y IaaS ofrecen diferentes ventajas, las cuales pueden ser aprovechadas en mayor medida si se conocen sus diferencias, similitudes, los requerimientos de la organización y para que se requiere dicho servicio.

- Las organizaciones que desean contratar servicios en la nube de manera segura y cuentan con un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001, deben incluir controles que permitan cumplir los criterios de seguridad propuestos en el presente trabajo, correspondientes a 6.1.4- Geolocalización de los datos, 6.1.5- Leyes y normativas de la industria, 6.1.9- Riesgos asociados con el proveedor de servicios en la nube y 6.1.12- Terceros y gestión de permisos. Debido a que dichos criterios no están contemplados o tienen un nivel de cumplimiento bajo dentro de dicho estándar.

- Las organizaciones con servicios en la nube que tienen implementado el estándar ISO/IEC 27017, deben tener en cuenta la implementación de controles adicionales para el cumplimiento de los criterios de seguridad propuestos en el presente trabajo, correspondientes a 6.1.4- Geolocalización de los datos, 6.1.5- Leyes y normativas de la

industria y 6.1.9- Riesgos asociados con el proveedor de servicios en la nube. Debido a que dichos criterios no están contemplados o tienen un nivel de cumplimiento bajo dentro de dicho estándar.

- Antes de contratar una organización en la nube se debe validar el nivel de cumplimiento de criterios de seguridad definidos en este trabajo con el fin de identificar los posibles riesgos a los cuales se puede encontrar expuesta la organización y su disposición a asumirlos.

- La primera actividad que debe llevar a cabo una organización antes de contratar servicios en la nube, es llevar a cabo un análisis de riesgos teniendo en cuenta los criterios de seguridad en computación en la nube definidos en este trabajo, esto teniendo en cuenta lo indicado en la ISO/IEC 27017.

- Con el fin de que las organizaciones puedan gestionar los riesgos en tecnologías de la información deben tener en cuenta los lineamientos establecidos en ISO/IEC 27005.

- Las empresas que se dedican a implementar aplicaciones en la nube deben tener en cuenta el estándar ISO/IEC 15408, el cual define los lineamientos para el cumplimiento de los criterios de seguridad respecto al desarrollo de software en computación en la nube con forme lo definido en la Tabla 5 Matriz de correlación de ISO/IEC15408:2009 con los criterios establecidos.

- Para profundizar en temas de desarrollo seguro en aplicaciones en la nube se deben tener en cuenta el estándar ISO/IEC15408 y las buenas practicas recopiladas en OWASP para el desarrollo seguro.

- La seguridad en la computación en la nube debe complementarse con un sistema de gestión de la seguridad de la información de tal manera que no solo se protejan los activos en la nube, sino todos los activos de la organización, con este fin se puede

utilizar el estándar ISO/IEC 27001.

- Cuando una organización desea implementar aplicaciones en la nube, debe tener en cuenta que modelo le permiten implementar la integridad, confidencialidad o disponibilidad; con el fin de facilitar la identificación de dichos modelos para su uso, el Anexo 5 detalla que modelo utilizar para asegurar la integridad, disponibilidad y confidencialidad.

- Para implementar la disponibilidad se deben tener en cuenta (Cloud Security Alliance, 2017) en lo referente al "Plano de gestión y continuidad de negocios" y los lineamientos de ISO/IEC 22301, ya que este pilar no se aborda en los modelos sino a través de estrategias para la continuidad del negocio.

- Para complementar la "Evaluación de riesgos de seguridad de la información en servicios en la nube" de ISO/IEC 27017, debe profundizarse con forme a lo explicado en (Department of Homeland Security, 2018) donde se tienen en cuenta aspectos como "Adquisición extranjera de CSP", "Aprovisionamiento malicioso de recursos", "Bloqueo del proveedor en la nube.", "Corte de servicio del proveedor de la nube", "Superficie de ataque aumentada debido a la tenencia múltiple", "Fuga de memoria en la infraestructura compartida" y "Modelo de negocio en la nube", adicionalmente se debe tener en cuenta (Cloud Security Alliance, 2017) donde se encuentran los temas relacionados con "Virtualización y contenedores".

- Cuando se está implementando ISO/IEC 27017, durante la revisión del "Cumplimiento con requisitos legales y contractuales" debe profundizarse en "Asuntos legales, contratos y documentos electrónicos" según lo establecido en (Cloud Security Alliance, 2017), "Coordinación con CSP para el cumplimiento de las leyes y reglamentos" según lo explicado en (Department of Homeland Security, 2018) y la privacidad según ISO/IEC 27018 y (International Organization for Standardization, 2009).

- Cuando se está implementando ISO/IEC 27001, durante la "Relaciones con Proveedores" debe profundizarse en este aspecto teniendo en cuenta lo estipulado en (Department of Homeland Security, 2018) acerca de "Administradores desconocidos", "Dependencias desconocidas del CSP", "Falta de conocimiento y control sobre la cadena de suministro." y "Mayor potencial para amenazas internas"

- Cuando se está implementando ISO/IEC 27001, durante la "Acciones para tratar riesgos y oportunidades" debe profundizarse teniendo en cuenta las referencia (Department of Homeland Security, 2018) donde se tienen en cuenta aspectos como "Adquisición extranjera de CSP", "Aprovisionamiento malicioso de recursos", "Bloqueo del proveedor en la nube.", "Corte de servicio del proveedor de la nube", "Superficie de ataque aumentada debido a la tenencia múltiple", "Fuga de memoria en la infraestructura compartida" y "Modelo de negocio en la nube", al igual que (Cloud Security Alliance, 2017) donde se encuentran los temas relacionados con "Virtualización y contenedores".

- Cuando se está implementando ISO/IEC 27001, durante la "Identificación de la legislación aplicable y de los requisitos contractuales" y "Privacidad y protección de información de datos personales" debe profundizarse en "Asuntos legales, contratos y documentos electrónicos" según lo establecido en (Cloud Security Alliance, 2017), "Coordinación con CSP para el cumplimiento de las leyes y reglamentos" según lo explicado en (Department of Homeland Security, 2018) y la privacidad según ISO/IEC 27018 y (International Organization for Standardization, 2009).

- Con el fin de asegurar "La Privacidad y protección de información de datos personales" deben tenerse en cuenta tanto la legislación de cada país como los lineamientos del estándar ISO/IEC27018.

- Cuando se van a contratar servicios en la nube es importante definir las responsabilidades entre las partes, a continuación, se presenta la tabla 7 con una

propuesta de responsabilidades entre cliente y proveedor según el servicio que se desea contratar.

Tabla 7. Definición de responsabilidades entre proveedor y cliente según servicios a contratar

	RESPONSABILIDADES	
SERVICIOS	Proveedor de la nube	Cliente
SaaS	Responsable de casi toda la seguridad Seguridad del perímetro El registro Monitoreo Auditoría La seguridad de la aplicación	Solo accede y administrar su uso de la aplicación, no puede alterar el funcionamiento de la aplicación. Mientras que el consumidor solo puede administrar la autorización y los derechos
PaaS	Seguridad de la plataforma. Seguridad fundamental Aplicación de parches Configuración central	Es responsable de todo lo que implementan en la plataforma incluida la forma en que configuran las características de seguridad ofrecidas
IaaS	Seguridad de la plataforma. Seguridad fundamental Aplicación de parches Configuración central Monitoreará su perímetro para detectar ataques	Responsable de todo lo que construyen en la infraestructura. Responsable de cómo definen e implementan la seguridad de su red virtual, según las herramientas disponibles en el servicio.

Fuente: (Propia)

- Los criterios aquí definidos se encuentran descritos a nivel general debido a la naturaleza del trabajo, si se requiere profundizar en cada uno de ellos se recomienda revisar los documentos oficiales enunciados en la Tabla 2 Criterios de seguridad y documentos de referencia.

7 CONCLUSIONES

A continuación, se presentan las conclusiones referentes al trabajo RECOMENDACIONES DE SEGURIDAD PARA LOS SERVICIOS DE COMPUTACIÓN EN LA NUBE, A PARTIR DE LOS ESTÁNDARES Y MODELOS DE SEGURIDAD DE LA INFORMACIÓN.

- Objetivamente se pueden definir criterios de seguridad debido a que se evidencian semejanzas entre los aspectos de seguridad identificados en los documentos analizados.

- Existen organizaciones a nivel mundial que ofrecen material gratuito, que permite entender, orientar e implementar las tecnologías de computación en la nube de manera segura, controlada y sostenible en cualquier organización, tal es el caso de Cloud Security Alliance (CSA).

- Una alternativa para implementar la seguridad en la computación en la nube es utilizar la documentación ofrecida por la organización CSA, la cual ofrece un alto nivel de detalle, sin embargo, por sí sola cumple con once (11) de los catorce (14) criterios de seguridad en computación en la nube definidos en este trabajo.

- Los aspectos de seguridad en computación en la nube del ministerio de defensa de los Estados Unidos tienen un cumplimiento de doce (12) de los catorce (14) criterios de seguridad en computación en la nube definidos en este trabajo, sin embargo, son expuesto como consideraciones sin un alto nivel de detalle, por lo tanto, deben complementarse con estándares u otras buenas prácticas.

- ISO/IEC 15408 por si solo cumple con ocho (8) de los catorce (14) criterios de seguridad en computación en la nube definidos en este trabajo, esto debido a que se encuentra enfocado en el desarrollo de productos informáticos, sin embargo, el

aseguramiento de aplicaciones es un factor importante para la seguridad en la nube.

- Las organizaciones que siguen los lineamientos del estándar ISO/IEC 15408 en el desarrollo de sus aplicaciones en la nube, tienen un mejor cumplimiento de los criterios de seguridad propuestos en el presente trabajo, debido a que el estándar define lineamientos para evaluar la seguridad y el desarrollo seguro de aplicaciones en la nube.

- La ISO/IEC 27017 Código de práctica para los controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube, definen los controles indicados en la norma ISO 27002, sin embargo, se profundizan en algunos de los controles con un enfoque a la computación en la nube, hecho que mejora el nivel de cumplimiento de los criterios de seguridad definidos en este trabajo en comparación con la ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información.

- Si bien es cierto, dentro de este trabajo se llevó a cabo el análisis del cumplimiento de los criterios de seguridad con respecto al estándar ISO/IEC27001:2013, ISO/IEC27017:2015 e ISO/IEC15408:2009, se recomienda ampliar el análisis con otros estándares de seguridad de la información, con el fin de mejorar el aporte a los criterios de la seguridad en la nube.

- Si bien es cierto existen estándares internacionales orientados a los controles de seguridad en la nube, en este trabajo se lleva a cabo un análisis y compilación para proponer los criterios de seguridad más representativos cuando una empresa quiere contratar servicios de en la nube, abordando de manera general cuales son los lineamientos que debería de cumplir al respecto.

- El estándar ISO/IEC 27001 presenta un cumplimento del 71% de los criterios con una calificación alta, el 7% de los criterios tiene controles asociados en el estándar que requieren la implementación de controles adicionales para mejorar su cumplimiento y el 21% de los criterios tienen un nivel de cumplimiento bajo.

- El estándar ISO/IEC 27017 presenta un cumplimento del 79% de los criterios con una calificación alta, el 14% de los criterios tiene controles asociados en el estándar que requieren la implementación de controles adicionales para mejorar su cumplimiento y el 7% de los criterios tienen un nivel de cumplimiento bajo.

- Se evidencia que la seguridad se puede implementar acudiendo a diferentes referentes como lo son las buenas prácticas, estándares y modelos, los cuales se pueden complementar entre sí para brindar un mayor nivel de aseguramiento.

- Al analizar los modelos de seguridad evidencia que no abarcan el pilar de la disponibilidad, para ello deben tenerse en cuenta los lineamientos relacionados con la continuidad del negocio que permiten establecer y garantizar el nivel de disponibilidad acorde a lo requerido por cada organización.

- La geolocalización de los datos es un aspecto importante para la seguridad en la nube, ya que tiene un gran impacto cuando ocurre un incidente informático y se requiere realizar un análisis forense y/o acceso a los medios físicos, puede existir implicaciones legales a tener en cuenta según el país donde se encuentren los datos y se pude perder el control, la privacidad o acceso a ellos.

BIBLIOGRAFÍA

Alert Logic. (2017). *2017 Cloud Security Report*. Retrieved from 2017 Cloud Security Report: https://www.alertlogic.com/resources/cloud-security-report-2017/?utm_source=evergage&utm_campaign=2017_Cloud_Security_Report&utm_medium=personalization

Cloud Security Alliance. (2016). The Treacherous 12 - Top Threats to Cloud Computing. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Cloud Security Alliance. (2017). *Security Guidance – For Critical Areas of Focus In Cloud Computing v4.* Retrieved from CSA: https://cloudsecurityalliance.org/guidance/#_overview

Cloud Security Alliance. (2019). https://cloudsecurityalliance.org/artifacts/cloud-security-complexity/. Retrieved from https://cloudsecurityalliance.org/artifacts/cloud-security-complexity/

Department of Homeland Security. (2018). Cloud Security Guidance. *Cloud Security Guidance - .gov Cloud Security Baseline*. U.S. Retrieved from https://www.us-cert.gov/sites/default/files/publications/Cloud_Security_Guidance-.gov_Cloud_Security_Baseline.pdf

Gartner Inc. (2019, 04 02). *Cyber attacks: A Cloud Security Report*. Retrieved from Gartner Inc.: https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

Harris, S. (n.d.). CISSP Exam Guide - Sixth Edition. In S. Harris, *CISSP Exam Guide - Sixth Edition.* McGraw-Hill.

International Organization for Standardization. (2009). ISO/IEC 15408-1:2009. *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*. Retrieved from https://www.iso.org/standard/50341.html

International Organization for Standardization. (2013). ISO/IEC 27001:2013. *Information technology -- Security techniques -- Information security management systems -- Requirements*. Retrieved from https://www.iso.org/standard/54534.html

International Organization for Standardization. (2014). ISO/IEC 17788:2014. *Information technology -- Cloud computing -- Overview and vocabulary*. Retrieved from https://www.iso.org/standard/60544.html

International Organization for Standardization. (2015). ISO/IEC 27017:2015. *Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Retrieved from https://www.iso.org/standard/43757.html

Jin B. Hong a, ∗. A. (2019). Systematic identification of threats in the cloud: A survey.

Marinescu, D. C. (2018). *Cloud Computing - Theory and Practice* (2nd Edition ed.). Morgan Kaufmann.

National Institute of Standads and Tecnology. (2011, Sep.). The NIST Definition of Cloud Computing. *The NIST Definition of Cloud Computing*. U.S. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

National Institute of Standards and Technology. (2011, July). NIST Cloud Computing Standards Roadmap. *NIST Cloud Computing Standards Roadmap*. U.S. Retrieved from https://csrc.nist.rip/library/NIST%20SP%20500-

291%20Cloud%20Computing%20Standards%20Roadmap,%202011-07-05.pdf

PaymentsCM LLP. (2015, 10 9). *Cyber attacks: A Cloud Security Report*. Retrieved from PaymentsCM LLP: https://www.paymentscardsandmobile.com/cyber-attacks-a-cloud-security-report/

Ph.D., M. P. (2012). Using the CSA Control Matrix and ISO 27017 controls to facilitate regulatory compliance in the cloud. Retrieved from https://docbox.etsi.org/workshop/2012/201201_securityworkshop/3_international_standardization/emc_csa_pohlmann.pdf

Rogers, P. (2019, Marzo 20). *Proofpoint releases Cloud Application Attack Snapshot research*. Retrieved from NTELLIGENT CISO: https://www.intelligentciso.com/2019/03/20/nigerian-cybercriminals-compromising-cloud-apps-with-data-breach/

School of Computing, Sathyabama Institute of Science and Technology. (2018). Recent security challenges in cloud computing. Chennai, India.